N Series Switches CLI

Reference Guide

Models: N5850-48S6Q; N8550-48B8C; N8550-32C

CLI REFERENCE GUIDE

content

1. Basic Commands····1

1.1 Overview····1

1.2 Basic Configuration Commands····1

1.2.1 command-privilege level····1

1.2.2 command authorization aaa method····2

1.2.3 command authorization config-command····2

1.2.4 clock set····4

1.2.5 clock summer-time····5

1.2.6 clock timezone····7

1.2.7 clear configuration····8

1.2.8 cls····9

1.2.9 configure····9

1.2.10 disable····10

1.2.11 enable····11

1.2.12 enable password····11

1.2.13 end····12

1.2.14 exit····13

1.2.15 help····14

1.2.16 hostname····15

1.2.17 list····15

1.2.18 management acl|management acl6····17

1.2.19 password····18

1.2.20 ping····19

1.2.21 ping6····20

1.2.22 quit····21

1.2.23 reboot····22

1.2.24 reboot {at|in}····22

1.2.25 reboot cancel····23

1.2.26 reset recycle····24

1.2.27 send message····25

1.2.28 show clock····26
1.2.29 show command-privilege····27
1.2.30 show history····27
1.2.31 show login-type count····28
1.2.32 show management acl····29
1.2.33 show module version····30
1.2.34 show privilege····31
1.2.35 show reboot····32
1.2.36 show system····33
1.2.37 show user config····34
1.2.38 show version····35
1.2.39 temporary-password····35
1.2.40 trace|trace6····36
1.2.41 user fail-count····37
1.2.42 show····38
1.2.43 user same-name-pwd····39
1.2.44 user reauth-interval····40
1.2.45 username····40
1.2.46 username domain····42
1.2.47 username group password····43
1.2.48 username online-count····44
1.2.49 user pwd-complex····44
1.2.50 user pwd-length····45
1.2.51 unlock-command vty····46
1.2.52 who····46
1.3 User Terminal Configuration Commands····47
1.3.1 case-sensitive····47
1.3.2 color····48
1.3.3 monitor····49
1.3.4 language····50
1.3.5 length····50

1.3.6 line console 51
1.3.7 line vty 52
1.3.8 login authentication 53
1.3.9 kill vty 54
1.3.10 show lines 55
1.3.11 timeout 56
1.4 File System Configuration Commands 57
1.4.1 cd 57
1.4.2 copy 58
1.4.3 del 59
1.4.4 dir 59
1.4.5 dir tree 61
1.4.6 execute 62
1.4.7 mkdir 63
1.4.8 move 63
1.4.9 pwd 64
1.4.10 remove 65
1.4.11 rename 66
1.4.12 rmdir 67
1.4.13 type 68
1.4.14 xcopy 72
1.4.15 zero 73
1.5 System Configuration File Commands 73
1.5.1 auth-degenerate 73
1.5.2 erase startup-config 74
1.5.3 show running-config 75
1.5.4 show startup-config 76
1.5.5 write file 80
1.6 File Uploading and Downloading Configuration Commands 81
1.6.1 tftp get 81
1.6.2 tftp put 82

1.6.3 tftpd····83
1.6.4 ftp delete····84
1.6.5 ftp get····85
1.6.6 ftp put····86
1.7 Telnet and SSH Configuration Commands····87
1.7.1 debug ssh····87
1.7.2 sshd····88
1.7.3 sshd auth····89
1.7.4 sshd login-grace-time····90
1.7.5 telnetd (IPv4)····90
1.7.6 telnet6d····91
1.7.7 telnet|telnet6····92
1.7.8 show ssh config····93
2. Ethernet Commands····94
2.1 Overview····94
2.2 Interface Configuration Commands····94
2.2.1 alias····94
2.2.2 duplex····94
2.2.3 error-down auto-recovery cause bpdu-protection interval····95
2.2.4 error-down auto-recovery cause mac-address-flapping····96
2.2.5 error-down auto-recovery cause storm-suppression interval····97
2.2.6 error-down auto-recovery cause transceiver-power-low interval····98
2.2.7 fec····99
2.2.8 flow-statistic include-interframe····100
2.2.9 interface····100
2.2.10 interface loopback····101
2.2.11 mtu····102
2.2.12 port-uniisolate····103
2.2.13 port-down holdoff-timer····103
2.2.14 priority····104
2.2.15 rate-limit····105

2.2.16 reset counter····106
2.2.17 show interface····107
2.2.18 show interface statistic····109
2.2.19 show interface unit-number····110
2.2.20 speed····111
2.2.21 storm-control····112
2.2.22 shutdown····113
2.2.23 switch {10gigaethernet|100gigaethernet}····114
2.2.24 port flow-stat interval····114
2.2.25 flow-stat interval····115
2.2.26 transceiver type····116
2.2.27 transceiver power low trigger error-down {enable|disable}····116
2.2.28 flush forward {enable|disable}····117
2.2.29 show flush····118
2.2.30 show flush interface····118
2.2.31 show storm-control····119
2.3 MAC Address Table Configuration Commands····120
2.3.1 mac aging-time····120
2.3.2 mac-address static····121
2.3.3 mac-address blackhole····122
2.3.4 mac-learning {enable|disable}····123
2.3.5 mac-address notification history-size····124
2.3.6 mac-learning disable action {forward|drop}····125
2.3.7 mac-address notification {add|remove|all}····125
2.3.8 mac-address notification interval····126
2.3.9 mac-address flapping detection {enable|disable}····127
2.3.10 mac-address flapping aging-time····128
2.3.11 mac-address flapping detection exclude-vlan····128
2.3.12 mac-address flapping detection vlan security-level····129
2.3.13 mac-address flapping quit-vlan recover-time····130
2.3.14 mac-address flapping action {quit-vlan|error-down}····131

2.3.15 mac-address flapping action priority 132
2.3.16 no mac-address 132
2.3.17 no mac-address {dynamic|static|security|sticky} 133
2.3.18 reset mac-address flapping record 134
2.3.19 reset mac-address notification history 135
2.3.20 show mac-address 136
2.3.21 show mac-address config 137
2.3.22 show mac-address total-number 138
2.3.23 show mac-address blackhole 139
2.3.24 show mac-address dynamic 139
2.3.25 show mac-address flapping record 141
2.3.26 show mac-address notification history 141
2.3.27 show mac info 142
2.3.28 show mac-address static 143
2.4 ARP Configuration Commands 144
2.4.1 arp detect-mode unicast 144
2.4.2 arp learning dhcp-trigger {enable|disable} 145
2.4.3 ip arp 145
2.4.4 ip arp detect {enable|disable} 146
2.4.5 ip arp detect-times 147
2.4.6 ip arp aging-time 148
2.4.7 flush arp 149
2.4.8 show arp-probe database 149
2.4.9 show arp-probe database verbose 150
2.4.10 show arp-probe global 152
2.4.11 show ip arp 153
2.5 ARP Proxy 154
2.5.1 debug arp-proxy 154
2.5.2 arp-proxy {enable|disable} 155
2.5.3 arp-proxy inner-sub-vlan-proxy {enable|disable} 156
2.5.4 arp-proxy inter-sub-vlan-proxy {enable|disable} 156

2.5.5 show arp-proxy config 157
2.5.6 show arp-proxy vlan 158
2.6 Link Aggregation Configuration Commands 159
2.6.1 active-linknumber 159
2.6.2 add 160
2.6.3 interface eth-trunk 161
2.6.4 join eth-trunk 162
2.6.5 lacp system-priority 163
2.6.6 load-balance 164
2.6.7 ip field 165
2.6.8 ipv6 field 166
2.6.9 l2 field 167
2.6.10 mode 168
2.6.11 schedule-profile 169
2.6.12 show interface eth-trunk verbose 170
2.6.13 show lacp config 171
2.6.14 show lacp eth-trunk 171
2.6.15 show lacp statistic interface eth-trunk 172
2.6.16 show lacp system 173
2.6.17 show schedule-profile 174
2.7 Mlag Configuration Commands 175
2.7.1 debug mlag 175
2.7.2 lacp mlag priority 176
2.7.3 lacp mlag system-id 177
2.7.4 mlag exclude interface 177
2.7.5 mlag-group 179
2.7.6 mlag interface eth-trunk 179
2.7.7 peerlink exclude 180
2.7.8 peerlink interface eth-trunk 181
2.7.9 priority 181
2.7.10 reset counter 182

2.7.11 security-key····183
2.7.12 show mlag····184
2.7.13 show mlag config····185
2.7.14 show mlag consistency····186
2.7.15 show mlag exclude interface····187
2.7.16 show mlag-group····187
2.7.17 source-address····188
2.7.18 stp v-stp enable····189
2.7.19 timer hello····190
2.7.20 timer hold-on-failure multiplier····191
2.7.21 up-delay····191
2.8 VLAN Configuration Commands····192
2.8.1 interface vlan····192
2.8.2 port default vlan····193
2.8.3 port hybrid vlan····194
2.8.4 port hybrid pvid····195
2.8.5 port link-type····195
2.8.6 port trunk allow-pass vlan····196
2.8.7 port trunk pvid····197
2.8.8 show interface vlan config····198
2.8.9 show vlan····199
2.8.10 show port vlan····200
2.8.11 tpid····201
2.8.12 unknown-multicast {forward|drop}····202
2.8.13 vlan unknown-multicast {forward|drop}····203
2.8.14 unknown-unicast {forward|drop}····204
2.8.15 vlan unknown-unicast {forwad|drop}····204
2.8.16 vlan-trunk {enable|disable}····205
2.8.17 vlan····206
2.8.18 no vlan····207
2.8.19 switch vlan····207

2.8.20 vlan normal 208
2.9 QinQ Configuration Commands 209
2.9.1 vlan-stacking {enable|disable} 209
2.9.2 dot1q-tunnel {enable|disable} 209
2.9.3 vlan-stacking vlan stack-vlan 210
2.9.4 show vlan-stacking 211
2.10 VLAN Mapping Configuration Commands 212
2.10.1 vlan-mapping {enable|disable} 212
2.10.2 vlan-mapping vlan map-vlan 213
2.10.3 show vlan-mapping 215
2.11 Port Security Configuration Commands 216
2.11.1 Port Security Configuration Commands 216
2.11.2 port-isolate mode 216
2.11.3 port-isolate group 217
2.11.4 join port-isolate group 217
2.11.5 add interface 218
2.11.6 show port-uniisolate interface 219
2.11.7 show port-isolategroup 220
2.11.8 show port-isolate information 221
2.11.9 show port-isolate config 222
2.12 MVRP Configuration Command 222
2.12.1 mvrp {start|stop} 222
2.12.2 mvrp gvrp-compliance {enable|disable} 223
2.12.3 mvrp {enable|disable} 224
2.12.4 mvrp timer leave 224
2.12.5 mvrp timer leave-all 225
2.12.6 mvrp timer join 226
2.12.7 mvrp registration 227
2.12.8 show mvrp 228
2.13 PVLAN Configuration Commands 229
2.13.1 no private-vlan 229

2.13.2 private-vlan association {add|remove}····230
2.13.3 private-vlan association····231
2.13.4 private-vlan host-association····232
2.13.5 private-vlan mapping····232
2.13.6 private-vlan mode····233
2.13.7 private-vlan {primary|isolated|community}····234
2.13.8 private-vlan primary-vid····235
2.13.9 show private-vlan interface····235
2.13.10 show private-vlan mapping····236
3. IP Commands····238
3.1 Overview····238
3.2 IPv4 Address Configuration Commands····238
3.2.1 ip address····238
3.2.2 mtu····239
3.2.3 ip prefix-list····239
3.2.4 ip forward-strict {enable|disable}····241
3.2.5 icmp redirect send {enable|disable}····241
3.2.6 show ip interface····242
3.2.7 show ip statistic····243
3.3 DHCP Configuration Commands····244
3.3.1 dhcp {start|stop}····244
3.3.2 dhcp address-check-time····244
3.3.3 option····245
3.3.4 option sub-option····246
3.3.5 option ipv6 rd ipv4 prefix-len prefix br····247
3.3.6 dhcp option82 circuit-id····248
3.3.7 dhcp option82 {enable|disable}····249
3.3.8 dhcp option82 {drop|keep|replace}····250
3.3.9 dhcp option82 remote-id····251
3.3.10 dhcp pool····252
3.3.11 dhcp relay server-ip····253

3.3.12 dhcp relay static-bind 253
3.3.13 dhcp relay user refresh-interval 254
3.3.14 dhcp server detect 255
3.3.15 dhcp server forbidden-ip 256
3.3.16 dhcp server option82 257
3.3.17 dhcp server static-bind 258
3.3.18 dns 259
3.3.19 gateway 259
3.3.20 ip dhcp 260
3.3.21 lease-time 261
3.3.22 lease-time day hour minute 262
3.3.23 network mask 263
3.3.24 no dhcp server bind all 264
3.3.25 no dhcp fake-server all 264
3.3.26 no dhcp server expired 265
3.3.27 no dhcp server conflict 266
3.3.28 no dhcp server dynamic-bind 266
3.3.29 reset dhcp relay statistic 267
3.3.30 reset dhcp server statistic 268
3.3.31 show dhcp 268
3.3.32 show dhcp bind-entry 269
3.3.33 show dhcp config 270
3.3.34 show dhcp fake-server 271
3.3.35 show dhcp lease-entry 271
3.3.36 show dhcp pool 272
3.3.37 show dhcp relay 273
3.3.38 show dhcp relay statistic 274
3.3.39 show dhcp relay user 275
3.3.40 show dhcp server 276
3.3.41 show dhcp server conflict 277
3.3.42 show dhcp server expired 277

3.3.43 show dhcp server statistic····· 278
3.3.44 show dhcp vlan config····· 279
3.4 DHCP Client Configuration Command····· 280
3.4.1 ip address dhcp {enable|disable}····· 280
3.4.2 ip address dhcp renew····· 280
3.4.3 ip address dhcp release····· 281
3.4.4 dhcp client auto-config mode····· 282
3.4.5 dhcp client ftp-name option····· 282
3.4.6 dhcp client ftp-password option····· 283
3.4.7 dhcp client ftp-server-ip option····· 284
3.4.8 dhcp client image-file option····· 285
3.4.9 dhcp client image-list option····· 285
3.4.10 dhcp client reboot-time option····· 286
3.4.11 dhcp client auth-message option····· 287
3.4.12 reset dhcp client statistic····· 287
3.4.13 show dhcp client····· 288
3.4.14 show dhcp client auto-config vlan····· 289
3.4.15 show dhcp client statistic····· 290
3.5 IPv6 Address Configuration Commands····· 291
3.5.1 flush ipv6 neighbor dynamic····· 291
3.5.2 flush ipv6 neighbor static····· 292
3.5.3 flush ipv6 neighbor all····· 292
3.5.4 ipv6 {enable|disable}····· 293
3.5.5 ipv6 address····· 293
3.5.6 ipv6 address eui-64····· 294
3.5.7 ipv6 address link-local····· 295
3.5.8 ipv6 address auto link-local····· 296
3.5.9 ipv6 description····· 297
3.5.10 ipv6 neighbor····· 297
3.5.11 ipv6 mtu····· 299
3.5.12 ipv6 nd lifetime····· 299

3.5.13 ipv6 prefix-list 300
3.5.14 ipv6 unicast-forwarding {enable|disable} 301
3.5.15 show ipv6 neighbor 302
3.5.16 show ipv6 interface 303
3.5.17 show ipv6 interface loopback 303
3.5.18 show ipv6 interface vlan 304
3.5.19 show ipv6 statistic interface vlan 305
3.5.20 show ipv6 statistic 306
3.5.21 show ipv6 route summary 307
3.5.22 show ipv6 neighbor 308
3.5.23 show ipv6 neighbor summary 308
3.5.24 show {ipv6|ip} prefix-list 309
4. Routing Commands 311
4.1 Overview 311
4.2 Static Route Configuration Commands 311
4.2.1 ip route-static 311
4.2.2 ipv6 route-static 313
4.2.3 ipv6 route-static interface vlan link-local 314
4.2.4 show ip config 315
4.2.5 show ip route 316
4.2.6 show ipv6 route 317
4.2.7 show {ip|ipv6} route statistic 318
4.2.8 show {ip|ipv6}route summary 319
4.3 RIP Configuration Command 320
4.3.1 debug rip 320
4.3.2 host-route 320
4.3.3 ip rip filter-policy export| import route-policy 321
4.3.4 ip rip authentication 322
4.3.5 ip rip default-metric 323
4.3.6 ip rip metric-in/out 324
4.3.7 ip rip passive-interface 325

4.3.8 ip rip receive-version····326
4.3.9 ip rip send-version····327
4.3.10 split-horizon {enable|disable}···· 328
4.3.11 ip rip timer basic····328
4.3.12 default-route originate {enable|disable}····329
4.3.13 poison-reverse {enable|disable}····330
4.3.14 network····331
4.3.15 router rip···· 332
4.3.16 validate-source-address···· 332
4.3.17 show ip rip····333
4.3.18 show ip rip resource····334
4.3.19 show ip rip config····335
4.3.20 show ip rip database····336
4.3.21 show ip rip interface····337
4.3.22 show ip rip neighbor····339
4.4 OSPFv2 Configuration Commands···· 340
4.4.1 filter route-policy····340
4.4.2 valid-ttl-hops····341
4.4.3 area range···· 341
4.4.4 area nssa range····343
4.4.5 area virtual-link···· 344
4.4.6 area authentication···· 345
4.4.7 area default-cost····347
4.4.8 area nssa default-cost····348
4.4.9 area nssa translator···· 349
4.4.10 area nssa····350
4.4.11 area te····351
4.4.12 area stub····352
4.4.13 area stub no-summary····353
4.4.14 area nssa no-summary····354
4.4.15 graceful-restart begin···· 354

4.4.16 graceful-restart helper····355
4.4.17 graceful-restart····356
4.4.18 ip ospf dead-interval····357
4.4.19 ip ospf hello-interval····357
4.4.20 ip ospf authentication····358
4.4.21 ip ospf bfd····359
4.4.22 ip ospf cost····360
4.4.23 ip ospf fast-change····361
4.4.24 ip ospf flooding-group····362
4.4.25 ip ospf if-type····362
4.4.26 ip ospf mtu····363
4.4.27 ip ospf mtu-ignore {enable|disable}····364
4.4.28 ip ospf passive-interface····365
4.4.29 ip ospf poll-interval····365
4.4.30 ip ospf priority····366
4.4.31 ip ospf retransmit-interval····367
4.4.32 ip ospf transmit-delay····368
4.4.33 network area····368
4.4.34 peer priority····369
4.4.35 redistribute····370
4.4.36 redistribute route-policy····372
4.4.37 redistribute metric····374
4.4.38 redistribute not-advertise|advertise····375
4.4.39 redistribute range····375
4.4.40 redistribute translate|no-translate····378
4.4.41 router-id····379
4.4.42 router ospf····380
4.4.43 reset ospf····381
4.4.44 reset ospf counters····381
4.4.45 spf-running-interval····382
4.4.46 show ip ospf area····383

4.4.47 show ip ospf bfd session 384
4.4.48 show ip ospf brief 385
4.4.49 show ip ospf config 386
4.4.50 show ip ospf database 386
4.4.51 show ip ospf graceful-restart 388
4.4.52 show ip ospf interface 389
4.4.53 show ip ospf neighbor 390
4.4.54 show ip ospf route 391
4.4.55 show ip ospf route count 392
4.4.56 show ip ospf statistic bfd 393
4.4.57 show ip ospf statistic global 394
4.4.58 show ip ospf statistic interface 396
4.4.59 show ip ospf statistic lsa 398
4.4.60 show ip ospf statistic memory 399
4.4.61 show ip ospf statistic neighbor 401
4.4.62 show ip ospf statistic route 402
4.4.63 show ip ospf statistic route process 403
4.4.64 show ip ospf statistic spf 404
4.4.65 show ip ospf trap 405
4.4.66 show ip ospf vitual interface 406
4.4.67 show ip ospf virtual neighbor 407
4.4.68 snmp-trap 408
4.4.69 opaque 409
4.4.70 bandwidth-reference 410
4.4.71 default-route-advertise always 410
4.4.72 loop-prevent 411
4.4.73 frr {enable|disable} 412
4.4.74 rfc1583 compatible 413
4.4.75 route-tag 413
4.4.76 preference 414
4.4.77 preference ase 415

4.5 OSPFv3 Configuration Command 416

4.5.1 area nssa 416

4.5.2 area nssa range 417

4.5.3 area range 418

4.5.4 area stub 419

4.5.5 area stub no-summary 420

4.5.6 area nssa no-summary 421

4.5.7 bandwidth-reference 421

4.5.8 graceful-restart 422

4.5.9 graceful-restart begin 423

4.5.10 graceful-restart helper 423

4.5.11 ipv6 ospf if-type 424

4.5.12 ipv6 ospf hello-interval 425

4.5.13 ipv6 ospf dead-interval 426

4.5.14 ipv6 ospf transmit-delay 426

4.5.15 ipv6 ospf area 427

4.5.16 ipv6 ospf bfd {enable|disable} 428

4.5.17 ipv6 ospf cost 429

4.5.18 ipv6 ospf peer 430

4.5.19 ipv6 ospf priority 431

4.5.20 ipv6 ospf passive-interface 431

4.5.21 ipv6 ospf retransmit-interval 432

4.5.22 ipv6 ospf mtu 433

4.5.23 ipv6 ospf mtu-ignore {enable|disable} 434

4.5.24 router ipv6 ospf 435

4.5.25 reset ipv6 ospf 435

4.5.26 reset ipv6 ospf counters 436

4.5.27 redistribute route-policy 437

4.5.28 router-id 439

4.5.29 show ipv6 ospf graceful-restart 440

4.5.30 show ipv6 ospf brief 440

4.5.31 show ipv6 ospf area····441
4.5.32 show ipv6 ospf bfd session····442
4.5.33 show ipv6 ospf config····443
4.5.34 show ipv6 ospf database····444
4.5.35 show ipv6 ospf database count····445
4.5.36 show ipv6 ospf interface····447
4.5.37 show ipv6 ospf neighbor····448
4.5.38 show ipv6 ospf route····449
4.5.39 show ipv6 ospf route count····449
4.5.40 show ipv6 ospf trap····450
4.5.41 filter route-policy····452
4.5.42 spf-running-interval····452
4.5.43 area nssa translator····453
4.6 BGP Configuration Commands····454
4.6.1 ipv4[ipv6]-family····454
4.6.2 aggregate····455
4.6.3 aggregate adminstatus····456
4.6.4 confederation identifier····457
4.6.5 confederation peer-as····458
4.6.6 cluster-id····459
4.6.7 community····460
4.6.8 dampening····461
4.6.9 debug bgp····462
4.6.10 default local-med····463
4.6.11 default local-preference····464
4.6.12 filter-policy {export|import} route-policy····464
4.6.13 filter-policy export····465
4.6.14 graceful-restart timer restart····466
4.6.15 graceful-restart timer selection-deferral····467
4.6.16 maximum load-balancing····468
4.6.17 network····468

4.6.18 neighbor ····· 469
4.6.19 neighbor advertisement-interval ····· 470
4.6.20 neighbor as-origin-interval ····· 471
4.6.21 neighbor connect-retry-interval ····· 472
4.6.22 neighbor ebgp-multihop ····· 473
4.6.23 neighbor keepalive-timer hold-timer ····· 474
4.6.24 neighbor next-hop-local ····· 475
4.6.25 neighbor route-policy {export|import} ····· 476
4.6.26 neighbor password ····· 477
4.6.27 neighbor remote-as ····· 478
4.6.28 neighbor restart ····· 479
4.6.29 neighbor route-reflector-client ····· 480
4.6.30 neighbor route-refresh ····· 481
4.6.31 neighbor send-community ····· 482
4.6.32 neighbor send-label ····· 483
4.6.33 neighbor send route-refresh ····· 484
4.6.34 neighbor shutdown ····· 485
4.6.35 neighbor update-source ····· 485
4.6.36 neighbor valid-ttl-hops ····· 486
4.6.37 neighbor allow-as-loop ····· 487
4.6.38 neighbor public-as-only ····· 488
4.6.39 preference ····· 489
4.6.40 router-id ····· 490
4.6.41 redistribute ····· 491
4.6.42 redistribute route-policy ····· 492
4.6.43 router bgp ····· 493
4.6.44 reset bgp ····· 494
4.6.45 show ip bgp route label ····· 495
4.6.46 show ip bgp aggregate ····· 495
4.6.47 show ip bgp config ····· 496
4.6.48 show ip bgp neighbor ····· 497

4.6.49 show ip bgp orf 498
4.6.50 show ip bgp resource 499
4.6.51 show ip bgp route 500
4.6.52 show ip bgp summary 501
4.6.53 tcp {server|client} {enable|disable} 502
4.6.54 update-size 503
4.7 ISIS Configuration Commands 504
4.7.1 area-authentication-mode 504
4.7.2 area-password 505
4.7.3 cost-style 505
4.7.4 debug isis 507
4.7.5 default-route-originate 507
4.7.6 domain-authentication-mode 508
4.7.7 domain-password 509
4.7.8 hostname 510
4.7.9 ignore-lsp-errors 511
4.7.10 ip router isis 511
4.7.11 is-type 512
4.7.12 isis bfd {enable|disable} 513
4.7.13 isis circuit-ext-domain 514
4.7.14 isis circuit-level 514
4.7.15 isis circuit-type 515
4.7.16 isis csnp-interval 516
4.7.17 isis default-metric 517
4.7.18 isis fast-sense neighbor 518
4.7.19 isis hello-interval 519
4.7.20 isis hello-multiplier 519
4.7.21 isis hello padding 520
4.7.22 isis mesh-group 521
4.7.23 isis password 522
4.7.24 isis passive-interface 523

4.7.25 isis priority 524
4.7.26 isis psnp-interval 524
4.7.27 isis three-way-handshake 525
4.7.28 isis wide-metric 526
4.7.29 lsp-generation max-interval 527
4.7.30 lsp-refresh-interval 528
4.7.31 max-lsp-lifetime 529
4.7.32 net 530
4.7.33 precedence 530
4.7.34 reset isis 531
4.7.35 redistribute 532
4.7.36 no redistribute route-policy 534
4.7.37 redistribute level-2 to level-1 534
4.7.38 router isis 535
4.7.39 router-id 536
4.7.40 set-overload-bit 537
4.7.41 snmp-trap 538
4.7.42 show ip isis 539
4.7.43 show ip isis bfd session 539
4.7.44 show ip isis config 540
4.7.45 show ip isis database 541
4.7.46 show ip isis database count 543
4.7.47 show ip isis database verbose 544
4.7.48 show ip isis hostname 546
4.7.49 show ip isis interface 546
4.7.50 show ip isis neighbor 548
4.7.51 show ip isis route 550
4.7.52 show ip isis spf-tree 551
4.7.53 show ip isis statistic 552
4.7.54 show ip isis virtual-system 554
4.7.55 summary-address 555

4.7.56 summary-prefix····556
4.7.57 traffic-engineer····557
4.7.58 timer spf····558
4.7.59 timer spf max-interval init-interval incr-interval····558
4.7.60 virtual-system····559
4.8 Routing Policy Configuration Commands····560
4.8.1 apply cost····560
4.8.2 apply cost-type····561
4.8.3 apply isis····562
4.8.4 apply local-preference····563
4.8.5 apply origin····563
4.8.6 apply ospf····564
4.8.7 apply preferred-value····565
4.8.8 apply tag····566
4.8.9 debug route-policy····567
4.8.10 match aspath····568
4.8.11 match cost····569
4.8.12 match ip|ipv6 filter-list····569
4.8.13 match ip-prefix····571
4.8.14 match ip {next-hop|route-source} ip-prefix····572
4.8.15 match ipv6 {address|next-hop|route-source} prefix-list····573
4.8.16 match ipv6 address prefix-list····574
4.8.17 match process····575
4.8.18 match route-type····576
4.8.19 match tag····577
4.8.20 route-policy····578
4.8.21 show route-policy····579
4.8.22 show route-policy config····581
4.8.23 show route-policy information····581
5. Multicast Commands····583
5.1 Overview····583

5.2 IGMP Snooping Configuration Commands 583

5.2.1 igmp-snooping drop 583

5.2.2 igmp-snooping {enable|disable} 583

5.2.3 igmp-snooping fast-leave 584

5.2.4 igmp-snooping fast-switch {enable|disable} 585

5.2.5 igmp-snooping fast-switch query {enable|disable} 586

5.2.6 igmp-snooping group-address mvlan 586

5.2.7 igmp-snooping max-response-time 587

5.2.8 igmp-snooping multicast user-vlan 588

5.2.9 igmp-snooping multicast-vlan 589

5.2.10 igmp-snooping mvlan 590

5.2.11 igmp-snooping forwarding-mode {ip|mac} 590

5.2.12 igmp-snooping group-limit 591

5.2.13 igmp-snooping group-policy filter-list 592

5.2.14 igmp-snooping querier {enable|disable} 593

5.2.15 igmp-snooping proxy-ip 593

5.2.16 igmp-snooping proxy-uplink-port 594

5.2.17 igmp-snooping query-interval 595

5.2.18 igmp-snooping report-suppress 596

5.2.19 igmp-snooping require-router-alert 597

5.2.20 igmp-snooping robust-count 597

5.2.21 igmp-snooping router-aging-time 598

5.2.22 igmp-snooping lastmember-querynumber 599

5.2.23 igmp-snooping lastmember-queryinterval 600

5.2.24 igmp-snooping send-query source-address 601

5.2.25 igmp-snooping {start|stop} 602

5.2.26 igmp-snooping static-group group-address mvlan 602

5.2.27 igmp-snooping static-group group-address mvlan user-vlan 603

5.2.28 igmp-snooping ssm-mapping {enable|disable} 604

5.2.29 igmp-snooping ssm-mapping filter-list source-address 605

5.2.30 igmp-snooping uplink-port 606

5.2.31 igmp-snooping uplink-port drop-report 607
5.2.32 igmp-snooping uplink-port-limit 607
5.2.33 igmp-snooping version 608
5.2.34 igmp-snooping workmode 609
5.2.35 reset igmp-snooping group 609
5.2.36 show igmp-snooping 610
5.2.37 show igmp-snooping config 611
5.2.38 show igmp-snooping egress-port 612
5.2.39 show igmp-snooping egress-port interface 612
5.2.40 show igmp-snooping egress-port mvlan 613
5.2.41 show igmp-snooping group 614
5.2.42 show igmp-snooping interface 615
5.2.43 show igmp-snooping mvlan 616
5.2.44 show igmp-snooping source-address 617
5.2.45 show igmp-snooping ssm-mapping 617
5.2.46 show igmp-snooping uplinkport 618
5.3 IGMP Configuration Command 619
5.3.1 igmp 619
5.3.2 igmp {enable|disable} 619
5.3.3 igmp fast-leave 620
5.3.4 igmp lastmember-queryinterval 621
5.3.5 igmp limit 622
5.3.6 igmp max-response-time 623
5.3.7 igmp timer other-querier-present 623
5.3.8 igmp general-query 624
5.3.9 general-query vlan 625
5.3.10 igmp group-policy filter-list 626
5.3.11 igmp require-router-alert 627
5.3.12 igmp robust-count 627
5.3.13 igmp send-router-alert 628
5.3.14 igmp {start|stop} 629

5.3.15 igmp static-group 630
5.3.16 igmp static-group egress-port 630
5.3.17 igmp static-group source 631
5.3.18 igmp static-group source egress-port 632
5.3.19 igmp ssm-mapping {enable|disable} 633
5.3.20 igmp ssm-mapping filter-list source-address 634
5.3.21 igmp timer query 635
5.3.22 igmp version 636
5.3.23 lastmember-queryinterval 636
5.3.24 limit 637
5.3.25 max-response-time 638
5.3.26 no igmp group vlan 639
5.3.27 no igmp group vlan source 639
5.3.28 no igmp group vlan source egress-port 640
5.3.29 require-router-alert 641
5.3.30 robust-count 642
5.3.31 send-router-alert 643
5.3.32 show igmp 643
5.3.33 show igmp config 644
5.3.34 show igmp egress-port 645
5.3.35 show igmp group 646
5.3.36 show igmp interface 647
5.3.37 show igmp source 649
5.3.38 show igmp ssm-mapping 650
5.3.39 timer other-querier-present 650
5.3.40 timer query 651
5.4 PIMv4 Configuration Command 652
5.4.1 assert-holdtime 652
5.4.2 accept-unknown-rp {enable|disable} 653
5.4.3 c-bsr admin-scope {enable|disable} 653
5.4.4 c-bsr send-interval 654

5.4.5 c-rp hold-time····655
5.4.6 c-rp send-interval····656
5.4.7 ip multicast-routing····656
5.4.8 ip pim {pim-sm|pim-dm}····657
5.4.9 ip pim bsr-boundary group····658
5.4.10 ip pim c-bsr····659
5.4.11 ip pim c-rp group priority····660
5.4.12 ip pim dr-priority····661
5.4.13 ip pim graft retry-time····661
5.4.14 ip pim hello-interval····662
5.4.15 ip pim hello-option holdtime····663
5.4.16 ip pim hello-option neighbor-tracking····664
5.4.17 ip pim hello-option override-interval····665
5.4.18 ip pim hello-option prune-delay····666
5.4.19 ip pim join-prune holdtime····667
5.4.20 ip pim join-prune interval····667
5.4.21 ip pim state-refresh-capable····668
5.4.22 pim····669
5.4.23 receive-check-neighbor····670
5.4.24 register externsion-checksum····670
5.4.25 register fragment····671
5.4.26 register mtu····672
5.4.27 register probe-interval····673
5.4.28 register suppression-timeout····673
5.4.29 reset pim routing-table····674
5.4.30 rp-address group····675
5.4.31 send-check-neighbor {enable|disable}····676
5.4.32 source-lifetime····676
5.4.33 state-refresh-interval····677
5.4.34 state-refresh-rate-limit····678
5.4.35 state-refresh-ttl····679

5.4.36 show ip pim····680
5.4.37 show ip pim bsr····681
5.4.38 show ip pim c-rp····681
5.4.39 show ip pim config····682
5.4.40 show ip pim interface····683
5.4.41 show ip pim neighbor····684
5.4.42 show ip pim route····684
5.4.43 show ip pim rp····685
5.4.44 show ip pim rp group····686
6. Service Security Commands····688
6.1 Overview····688
6.2 IP Address Prefix-list Configuration Command····688
6.2.1 {ip|ipv6} prefix-list····688
6.2.2 {ip|ipv6} prefix-list greater-equal····689
6.2.3 {ip|ipv6} prefix-list less-equal····691
6.2.4 {ip|ipv6} prefix-list greater-equal less-equal····692
6.2.5 no {ip|ipv6} prefix-list····694
6.2.6 show {ip|ipv6} prefix-list····695
6.2.7 show ip prefix-list information····695
6.2.8 ACL Configuration Commands····696
6.2.9 filter-list····696
6.2.10 filter-list {in|out}····698
6.2.11 filter action {permit|deny}····699
6.2.12 filter ip····699
6.2.13 filter ip dscp····700
6.2.14 filter ip fragment····701
6.2.15 filter ip precedence····702
6.2.16 filter ip precedence fragment····703
6.2.17 filter ip proto-type····704
6.2.18 filter ip tos····705
6.2.19 filter ip ttl····706

6.2.20 filter icmp 707
6.2.21 filter igmp 708
6.2.22 filter tcp 709
6.2.23 filter udp 710
6.2.24 filter mac 712
6.2.25 no filter 713
6.2.26 show filter-list 714
6.2.27 show filter-list brief 714
6.2.28 show filter-list config 715
6.2.29 show filter-list interface 716
6.2.30 show filter-list name 717
6.2.31 show filter-list statistic 717
6.2.32 counter 718
6.2.33 show counter 719
6.3 IPv6 ACL Configuration Commands 720
6.3.1 filter icmp6 720
6.3.2 filter igmp6 721
6.3.3 filter ip6 722
6.3.4 filter ip6 hop-limit 723
6.3.5 filter ip6 next-header 723
6.3.6 filter tcp6 724
6.3.7 filter udp6 726
6.4 Traffic Policing and Traffic Shaping Configuration Commands 727
6.4.1 filter action counter 727
6.4.2 filter action mirror group 728
6.4.3 filter meter 729
6.4.4 filter action cpu 730
6.4.5 filter action {cos|precedence|prioriy} 730
6.4.6 filter action dscp 731
6.4.7 filter car outaction drop 732
6.4.8 filter outaction 733

6.4.9 meter····734
6.4.10 no filter action····736
6.4.11 reset counter filter-list····736
6.4.12 show meter····737
6.4.13 show meter config····738
6.5 Queue Scheduling and Congestion Control Configuration Commands····739
6.5.1 cos priority queue····739
6.5.2 cos queue weight····740
6.5.3 cos scheduling····740
6.5.4 show cos····741
6.6 DHCP Snooping Configuration Commands····742
6.6.1 dhcp-snooping alarm untrust-replay {enable|disable}····742
6.6.2 dhcp-snooping alarm untrust-replay threshold····743
6.6.3 dhcp-snooping binding····744
6.6.4 dhcp-snooping check mac-address····745
6.6.5 dhcp-snooping check user-bind {enable|disable}····746
6.6.6 dhcp-snooping {enable|disable}····747
6.6.7 dhcp-snooping max-user-number····747
6.6.8 dhcp-snooping option82 circuit-id····748
6.6.9 dhcp-snooping option82 {circuit-id|remote-id} format····749
6.6.10 dhcp-snooping option82 {drop|keep|append}····751
6.6.11 dhcp-snooping option82 {enable|disable}····752
6.6.12 dhcp-snooping option82 remote-id····752
6.6.13 dhcp-snooping option82 sub-option9····753
6.6.14 dhcp-snooping relay server-ip····754
6.6.15 dhcp-snooping relay-agent-ip····755
6.6.16 dhcp-snooping sticky-mac {enable|disable}····756
6.6.17 dhcp-snooping server detect····756
6.6.18 dhcp-snooping {start|stop}····757
6.6.19 dhcp-snooping {trust|untrust}····758
6.6.20 dhcp-snooping trust interface····758

6.6.21 reset dhcp-snooping statistic 759
6.6.22 show dhcp-snooping binding 760
6.6.23 show dhcp-snooping config 761
6.6.24 show dhcp-snooping fake-server 761
6.6.25 show dhcp-snooping interface 762
6.6.26 show dhcp-snooping statistic 763
6.7 IP Source Guard Configuration Commands 764
6.7.1 ip source check user-bind {enable|disable} 764
6.7.2 ip source check user-bind alarm {enable|disable} 765
6.7.3 ip source check user-bind alarm threshold 766
6.7.4 ip source check user-bind check-item 766
6.7.5 reset ip source statistic check user-bind 767
6.7.6 show ip source check user-bind 768
6.7.7 show user-bind 769
6.7.8 show user-bind config 770
6.7.9 user-bind alarm untrust-user 770
6.7.10 user-bind black-list 771
6.7.11 user-bind static ip|ip6 mac 772
6.8 AAA/Radius Configuration Commands 773
6.8.1 aaa 773
6.8.2 aaa authorization console 774
6.8.3 aaa {authentication|account} 774
6.8.4 aaa authentication enable method 776
6.8.5 aaa authorization method 777
6.8.6 account realtime 778
6.8.7 no aaa method 779
6.8.8 no radius-server 779
6.8.9 no server-group 780
6.8.10 no tacacs-server 781
6.8.11 radius-server acct-port 781
6.8.12 radius-server auth-port 782

6.8.13 radius-server deadtime····783
6.8.14 radius-server {ip-address|ip6-address} key····784
6.8.15 radius-server {ip-address|ip6-address} key auth-port acct-port····785
6.8.16 radius-server max-retransmit····786
6.8.17 radius-server retransmit-interval····786
6.8.18 radius-server {src-ip|src-ipv6}····787
6.8.19 reset server statistic····788
6.8.20 sever-group {radius-server|tacacs-server}····789
6.8.21 show aaa····790
6.8.22 show aaa config····790
6.8.23 show aaa method····791
6.8.24 show aaa server····792
6.8.25 show aaa server-group····793
6.8.26 show aaa tacacs-server statistic····794
6.8.27 show radius client····795
6.8.28 tacacs-server deadtime····796
6.8.29 tacacs-server {ip-address|ip6-address} key····797
6.8.30 tacacs-server {ip-address|ipv6-address} key port single-connection····798
6.8.31 tacacs-server port····799
6.8.32 tacacs-server single-connection {enable|disable}····799
6.8.33 tacacs-server {src-ip|src-ipv6}····800
6.8.34 tacacs-server timeout····801
6.9 802.1x Configuration Commands····802
6.9.1 dot1x aaa-account····802
6.9.2 dot1x aaa-authentication····803
6.9.3 dot1x authentication auth-method····803
6.9.4 dot1x authentication client-timeout····804
6.9.5 dot1x authentication logical-port····805
6.9.6 dot1x authentication max-request····806
6.9.7 dot1x authentication max-user····807
6.9.8 dot1x authentication quiet-period····807

6.9.9 dot1x authentication reauthenticate-period····808
6.9.10 dot1x authentication server-timeout····809
6.9.11 dot1x authentication tx-period····810
6.9.12 dot1x default aaa-account····811
6.9.13 dot1x default aaa-authentication····811
6.9.14 dot1x default supplicant-support····812
6.9.15 dot1x default vlan-assignment-mode····813
6.9.16 dot1x {enable|disable}····813
6.9.17 dot1x guest vlan····814
6.9.18 dot1x interface aaa····815
6.9.19 dot1x link-mode····816
6.9.20 dot1x mac-delete-notify····816
6.9.21 dot1x reauthenticate····817
6.9.22 dot1x {start|stop}····818
6.9.23 dot1x supplicant-support····819
6.9.24 dot1x vlan-assignment-mode····819
6.9.25 no dot1x authentication user all····820
6.9.26 no dot1x interface user all····821
6.9.27 show dot1x authentication user····821
6.9.28 show dot1x config····822
6.9.29 show dot1x interface····823
6.9.30 show dot1x statistic····824
6.9.31 show dot1x statistic {10gigaethernet|100gigaethernet}····825
6.10 Storm Suppression Configuration Commands····826
6.10.1 storm-suppression log {enable|disable}····826
6.10.2 storm-suppression trap {enable|disable}····827
6.10.3 storm-suppression {multicast|broadcast|dlf} min-rate max-rate····828
6.10.4 storm-suppression action {block|error-down|none}····829
6.10.5 storm-suppression interval····829
6.10.6 show storm-suppression interface····830
6.10.7 show storm-suppression config····831

7. Reliability Commands 833

7.1 Overview 833

7.2 MSTP Configuration Commands 833

7.2.1 no stp instance 833

7.2.2 show stp 833

7.2.3 show stp brief 835

7.2.4 show stp config 835

7.2.5 show stp information 836

7.2.6 show stp instance interface 837

7.2.7 show stp interface 839

7.2.8 show stp interface {10gigaethernet|100gigaethernet|eth-trunk} 839

7.2.9 show stp tc-bpdu statistic 841

7.2.10 show stp topology-change 842

7.2.11 stp 842

7.2.12 stp bpdu-filter 843

7.2.13 stp bpdu-guard 844

7.2.14 stp config-name 845

7.2.15 stp {enable|disable} 845

7.2.16 stp edge-port 846

7.2.17 stp edge-default 847

7.2.18 stp forward-delay 847

7.2.19 stp hello-time 848

7.2.20 stp instance path-cost 849

7.2.21 stp instance priority (in the STP Configuration View) 850

7.2.22 stp instance priority (interface configuration view) 851

7.2.23 stp instance vlan 852

7.3 stp link-detection 852

7.3.1 stp loop-guard 853

7.3.2 stp max-age 854

7.3.3 stp max-hop 855

7.3.4 stp mcheck 855

7.3.5 stp migration-time····· 856
7.3.6 stp mode····· 857
7.3.7 stp path-cost····· 858
7.3.8 stp pathcost-standard····· 858
7.3.9 stp point-to-point····· 859
7.3.10 stp priority (STP configuration view)····· 860
7.3.11 stp priority (interface configuration view)····· 861
7.3.12 stp reset statistic····· 861
7.3.13 stp revision-level····· 862
7.3.14 stp root-guard····· 863
7.3.15 stp tc-flush-arp····· 863
7.3.16 stp tc-hold-off····· 864
7.3.17 stp tc-protection····· 865
7.3.18 stp tc-protection threshold····· 866
7.3.19 stp timer-factor····· 867
7.3.20 stp transmit-limit····· 867
7.3.21 stp trap····· 868
7.4 G.8032 Configuration Commands····· 869
7.4.1 g8032····· 869
7.4.2 g8032 instance mip-port····· 869
7.4.3 g8032 instance {port1|port2} (in the Interface Configuration View)····· 870
7.4.4 g8032 instance {add|remove} mip-port····· 871
7.4.5 g8032 instance {port1|port2} (in the G8032 Configuration View)····· 872
7.4.6 g8032 instance {port1|port2} fs····· 872
7.4.7 g8032 instance {port1|port2} ms····· 873
7.4.8 g8032 instance channel····· 874
7.4.9 g8032 instance clear····· 874
7.4.10 g8032 instance mel····· 875
7.4.11 g8032 instance mode····· 876
7.4.12 g8032 instance role····· 877
7.4.13 g8032 instance rpl····· 877

7.4.14 g8032 instance vc-holdoff-timer····878
7.4.15 g8032 instance vc-mel····879
7.4.16 g8032 instance vc-mep {port1|port2|none}····880
7.4.17 g8032 instance version····880
7.4.18 g8032 instance virtual-channel····881
7.4.19 g8032 instance vlan····882
7.4.20 g8032 instance wtr-timer····882
7.4.21 g8032 instance guard-timer····883
7.4.22 g8032 instance hold-off-timer····884
7.4.23 g8032 trap {enable|disable}····885
7.4.24 g8032 vs-switch {enable|disable}····885
7.4.25 no g8032 instance····886
7.4.26 show g8032····887
7.4.27 show g8032 instance····887
7.4.28 show g8032 instance interface····888
7.4.29 show g8032 interface····889
7.5 UDLD Configuration Commands····890
7.5.1 udld work-mode····890
7.5.2 udld uni-shutdown····890
7.5.3 udld advertise-interval····891
7.5.4 udld trap {enable|disable}····892
7.5.5 udld {enable|disable}····893
7.5.6 udld aggressive {enable|disable}····893
7.5.7 show udld local····894
7.5.8 show udld interface····895
7.5.9 show udld peer····895
7.5.10 show udld config····896
7.6 FLINK Configuration Commands····897
7.6.1 join mlink group····897
7.6.2 join flink group····898
7.6.3 manual-change····899

7.6.4 mlink group····899
7.6.5 add interface {10gigaethernet|100gigaethernet } role {master|slave|sender}····900
7.6.6 add interface {10gigaethernet|100gigaethernet|ethernet| xgigaethernet } role {uplink|downlink}····901
7.6.7 protect-vlan····902
7.6.8 receive-timeout····903
7.6.9 reverse {enable|disable}····904
7.6.10 reverse time····905
7.6.11 flink group····905
7.6.12 flink group send-vlan····906
7.6.13 send-interval····907
7.6.14 show mlink config····908
7.6.15 show mlink group····909
7.6.16 show mlink interface····910
7.6.17 show flink config····910
7.6.18 show flink group····911
7.6.19 show flink interface····912
7.6.20 type {single|double}····913
7.6.21 snmp-trap {enable|disable}····914
7.7 BFD Configuration Commands····914
7.7.1 bfd authentication····914
7.7.2 bfd {enable|disable}····915
7.7.3 bfd min-echo····916
7.7.4 bfd min-tx min-rx multiplier····917
7.7.5 bfd role····918
7.7.6 bfd {start|stop}····919
7.7.7 bfd trap····919
7.7.8 bfd track····920
7.7.9 show bfd config····921
7.7.10 show bfd interface····922
7.7.11 show bfd session····923
7.7.12 show bfd track····924

7.8 VRRP Configuration Commands 925

7.8.1 ip vrrp 925

7.8.2 ip vrrp snmp-trap {enable|disable} 926

7.8.3 ip vrrp advertise-interval 926

7.8.4 ip vrrp associate-address 927

7.8.5 ip vrrp authentication-mode 928

7.8.6 ip vrrp check-ttl {enable|disable} 929

7.8.7 ip vrrp gratuitous-arp {enable|disable} 930

7.8.8 ip vrrp gratuitous-arp timeout 931

7.8.9 ip vrrp holding-multiplier 931

7.8.10 ip vrrp preempt 932

7.8.11 ip vrrp preempt timer delay 933

7.8.12 ip vrrp priority 934

7.8.13 ip vrrp role admin 935

7.8.14 ip vrrp track admin-vrrp interface vlan 935

7.8.15 ip vrrp track bfd-session 936

7.8.16 ip vrrp track interface vlan 937

7.8.17 ip vrrp admin-vrrp associate-vrrp interface vlan 938

7.8.18 reset ip vrrp statistic 939

7.8.19 show ip vrrp 939

7.8.20 show ip vrrp admin-vrrp 940

7.8.21 show ip vrrp associate interface 941

7.8.22 show ip vrrp binding 942

7.8.23 show ip vrrp binding admin-vrrp interface 943

7.8.24 show ip vrrp config 944

7.8.25 show ip vrrp interface vlan 944

7.8.26 show ip vrrp statistic 946

8. Device Management Commands 948

8.1 Overview 948

8.2 Hardware Configuration Commands 948

8.2.1 cpu low-threshold 948

8.2.2 cpu monitor····949
8.2.3 cpu trap····949
8.2.4 fan monitor····950
8.2.5 fan threshold····951
8.2.6 fan all level····952
8.2.7 fan all mode····952
8.2.8 memory high-threshold····953
8.2.9 memory low-threshold····954
8.2.10 memory monitor····955
8.2.11 memory trap····955
8.2.12 show cpu statistic····956
8.2.13 show fan····959
8.2.14 show memory pool····960
8.2.15 show temperature····963
8.2.16 show temperature config····963
8.2.17 temperature monitor····964
8.2.18 temperature threshold····965
8.2.19 temperature trap····965
8.3 Mirror Configuration Commands····966
8.3.1 mirror group (Local Mirror)····966
8.3.2 show mirror config····967
8.3.3 show mirror group····968
8.3.4 show mirror interface····969
8.4 NTP Configuration Commands····969
8.4.1 debug ntp····969
8.4.2 ntp····970
8.4.3 ntp broadcast-client····971
8.4.4 ntp multicast-client····972
8.4.5 ntp broadcast-server····972
8.4.6 ntp multicast-server····973
8.4.7 show ntp····975

8.4.8 show ntp service 975
8.4.9 show ntp service verbose 976
8.4.10 show ntp config 979
8.4.11 authentication {enable|disable} 980
8.4.12 authentication-keyid 980
8.4.13 client update-interval 981
8.4.14 ntp unicast-peer 982
8.4.15 master 984
8.4.16 ntp unicast-server 985
8.4.17 oncesync { enable | disable } 987
8.4.18 server broadcast-interval 988
8.4.19 stratum 988
8.4.20 trusted-keyid {enable|disable} 989
9. VXLAN Configuration Commands 991
9.1 Overview 991
9.1.1 bridge-domain (global configuration view) 991
9.1.2 vxlan vni 994
9.1.3 interface nve 995
9.1.4 vni ucast-peer 995
9.1.5 tunnel source 996
9.1.6 encapsulation {dot1q|untag|qinq|default} 997
9.1.7 bridge-domain bind (layer 2 sub-interface view) 998
9.1.8 encapsulation dot1q 999
9.1.9 encapsulation qinq vid ce-vid 1000
9.1.10 debug vxlan 1000
9.1.11 show bridge-domain 1001
9.1.12 show vxlan vni 1002
9.1.13 show vxlan resource 1003
9.1.14 show nve peer 1004
9.1.15 show interface nve 1004
9.1.16 show ip arp vxlan 1005

9.1.17 show ip bgp evpn route····· 1006
9.1.18 show ipv6 nd l2-proxy····· 1007
9.1.19 unknown-ucast {forward|drop}····· 1007
9.1.20 vxlan anycast-gateway {enable|disable}····· 1008
9.1.21 debug ipv6 nd l2-proxy····· 1009
9.1.22 reset vxlan statistics peer-ip····· 1009
9.1.23 debug trace vxlan····· 1010
9.1.24 ping vxlan vni source peer····· 1011
9.1.25 trace vxlan vni source peer····· 1012
9.1.26 rewrite egress vid····· 1013
9.1.27 rewrite no-action····· 1014
9.1.28 rewrite pop double····· 1014
9.1.29 debug evpn····· 1015
9.1.30 debug bgp····· 1016
9.1.31 evpn····· 1017
9.1.32 evpn-family····· 1017
9.1.33 evpn route-distinguisher····· 1018
9.1.34 evpn vpn-target····· 1019
9.1.35 neighbor enable····· 1020
9.1.36 vni replication-protocol····· 1021
9.1.37 vxlan vni····· 1022
9.1.38 show evpn····· 1022
9.1.39 show evpn vpn-target····· 1023
10. VPN Commands····· 1025
10.1 Overview····· 1025
10.2 L3VPN Configuration Commands····· 1025
10.2.1 debug l3vpn····· 1025
10.2.2 description····· 1025
10.2.3 ip binding vpn-instance····· 1026
10.2.4 ipv4-family|ipv6-family····· 1027
10.2.5 vpn-target····· 1027

10.2.6 route-distinguisher 1029
10.2.7 show ip vpn-instance 1030
10.2.8 show ip vpn-instance verbose 1031
10.2.9 show ip vpn-instance config 1032
10.2.10 show ip vpn-instance import-vt 1033
10.2.11 route-distinguisher 1034
11. Operation and Maintenance Commands 1036
11.1 Overview 1036
11.2 RMON Configuration Commands 1036
11.2.1 rmon alarm 1036
11.2.2 rmon event 1037
11.2.3 show rmon alarm 1038
11.2.4 show rmon config 1039
11.2.5 show rmon event 1040
11.2.6 show rmon history 1041
11.2.7 show rmon history statistics 1042
11.2.8 show rmon log 1043
11.2.9 show rmon statistics 1044
11.3 SNMP Configuration Commands 1045
11.3.1 show snmp agent 1045
11.3.2 show snmp community 1046
11.3.3 show snmp config 1047
11.3.4 show snmp group 1048
11.3.5 show snmp statistic 1048
11.3.6 show snmp trap-server 1050
11.3.7 show snmp user 1051
11.3.8 show snmp view 1051
11.3.9 snmp auth-trap 1052
11.3.10 snmp bulk max-varbind 1053
11.3.11 snmp community 1053
11.3.12 snmp contact 1054

11.3.13 snmp fail-count····· 1055
11.3.14 snmp group····· 1056
11.3.15 snmp location····· 1057
11.3.16 snmp|snmp6 port····· 1057
11.3.17 snmp reauth-interval····· 1058
11.3.18 snmp rw-community····· 1059
11.3.19 snmp|snmp6 trap-server····· 1060
11.3.20 snmp trap-source····· 1061
11.3.21 snmp user····· 1062
11.3.22 snmp version····· 1063
11.3.23 snmp view····· 1063
11.4 LLDP Configuration Commands····· 1064
11.4.1 lldp tx-interval····· 1064
11.4.2 lldp tx-hold····· 1065
11.4.3 lldp reinit-delay····· 1066
11.4.4 lldp tx-delay····· 1066
11.4.5 lldp notification-interval····· 1067
11.4.6 lldp admin-status····· 1068
11.4.7 lldp notification {enable|disable}····· 1069
11.4.8 lldp management-address····· 1069
11.4.9 lldp basic-tlv-tx····· 1070
11.4.10 reset lldp counter····· 1071
11.4.11 show lldp interface····· 1072
11.4.12 show lldp statistic····· 1073
11.4.13 show lldp remote····· 1074
11.4.14 show lldp local····· 1074
11.4.15 show lldp config····· 1076
11.4.16 show lldp remote interface····· 1076
11.4.17 show lldp config interface····· 1077
11.4.18 show lldp local interface····· 1078

1. Basic Commands

1.1 Overview

This chapter introduces the basic configuration of the N-series switch.

1.2 Basic Configuration Commands

1.2.1 command-privilege level

Function

The **command-privilege level** command modifies the default priority of a command line.
The **no command-privilege level** command cancels the default priority modification of a command line.

Format

- **command-privilege level** *level-value* **view** *VIEW COMMAND*
- **no command-privilege level** *level-value* **view** *VIEW COMMAND*

Parameters

Parameters	Description	Value
level-value	Specifies the command level.	The value is an integer in the range from 0 to 15.
VIEW	Specifies the command configuration view.	aaa|configure|enable|vlanif|eth-trunk|vlan|ethernet|tunnelif|nullif|loopbackif
COMMAND	Specifies the detailed configuration command.	The value is a character string.

Default Value

None

View

Global configuration view

Usage Guidelines

The command level ranges from 0 to 15. 15 indicates the administrator authority and 0 indicates the visitor authority.

Example

Set the level of the command "command-privilege level 3 view configure aaa" in the AAA view to 3.

```
switch(config)#command-privilege level 3 view configure aaa
switch(config)#
```

1.2.2 command authorization aaa method

Function

The **command authorization aaa method** command sets the command authorization method on a terminal.
The **no command authorization aaa method** command cancels the configured command authorization method on a terminal.

Format

- **command authorization level-value aaa method name**
- **no command authorization level-value aaa method**

Parameters

Parameters	Description	Value
name	Specifies an AAA authorization method name.	The value is a character string.
level-value	Specifies a privilege level.	It is an integer, and the value ranges from 0 to 15.

Default Value

None

View

Line configuration view

Usage Guidelines

None

Example

```
switch(config-line)#command authorization 3 aaa method 111a
switch(config-line)#
```

1.2.3 command authorization config-command

Function

The **command authorization config-command** command configures authorization for commands in the global configuration view on the terminal.
The **no command authorization config-command** command disables authorization for commands in the global configuration view on the terminal.

Format

- **command authorization config-command**
- **no command authorization config-command**

Parameters

None

Default Value

By default, command authorization is disabled.

View

Line configuration view

Usage Guidelines

None

Example

#Configures authorization for commands in the global configuration view on the terminal.

```
switch(config-line)#command authorization config-command
switch(config-line)#
```

1.2.4 clock set

Function

The **clock set** command sets the current date and time on the switch.

Format

- **clock set** *HH:MM:SS DD MM YYYY*
- **clock set** *HH:MM:SS YYYY/MM/DD*

Parameters

Parameters	Description	Value
HH:MM:SS	Specifies the current time on the switch. HH specifies hours. MM specifies minutes. SS specifies seconds.	HH is an integer in the range from 0 to 23. MM is an integer in the range from 0 to 59. SS is an integer in the range from 0 to 59.
DD	Specifies the current date on the switch.	The value is an integer in the range from 1 to 31.
MM	Specifies the current month on the switch.	The value is an integer in the range from 1 to 12.
YYYY	Specifies the current year on the switch.	The value is an integer in the range from 2001 to 2036.

Default Value

None

View

Global configuration view

Usage Guidelines

In an environment that requires the absolute time, you must set the current date and time on the switch.
The time must be in the 24-hour format. If you do not specify MM:SS, the value is 00:00. You must set the value of HH (at least one digit). For example, if you enter 0, the time is 00:00:00.
The year in the date must be four digits.

Example

Set the current date and time to 2019-3-31 16:10:19.

```
switch(config)#clock set 16:10:19 31 3 2019
switch(config)#
```

1.2.5 clock summer-time

Function

The **clock summer-time** command sets the name, start time, and end time of daylight saving time.
The **no clock summer-time** command cancels the configuration of daylight saving time.

Format

- **clock summer-time** *summer-time-name* **date** *start-hour.start-minutes start-day start-month start-year end-hour.end-minutes end-day end-month end-year*
- **clock summer-time** *summer-time-name* **date** *start-hour.start-minutes start-year/start-month/start-day end-hour.end-minutes end-year/end-month/ end-day*
- **clock summer-time** *summer-time-name* **recurring** { **first** | **second** | **third** | **fourth** | **fifth** | **last** } { **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday** | **sunday** } { **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december** } *start-hour.start-minutes* { **first** | **second** | **third** | **fourth** | **fifth** | **last** } { **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday** | **sunday** } { **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december** } *end-hour.end-minutes*
- **no clock summer-time**

Parameters

Parameters	Description	Value
summer-time-name	Specifies the name of the daylight saving time zone.	The value is a string of 1 to 32 characters.
date	Specifies the absolute daylight saving time.	-
recurring	Specifies the periodic daylight saving time.	-
start-hour	Specifies the start hour.	The value is an integer in the range from 0 to 23.
start-minutes	Specifies the start minute.	The value is an integer in the range from 0 to 59.
start-day	Specifies the start day.	The value is an integer in the range from 1 to 31.
start-month	Specifies the start month.	The value is an integer in the range from 1 to 12.
start-year	Specifies the start year.	The value is an integer in the range from 2001 to 2036.
end-hour	Specifies the end hour.	The value is an integer in the range from 0 to 23.
end-minutes	Specifies the end minute.	The value is an integer in the range from 0 to 59.
end-day	Specifies the end day.	The value is an integer in the range from 1 to 31.
end-month	Specifies the end month.	The value is an integer in the range from 1 to 12.

Parameters	Description	Value
end-year	Specifies the end year.	The value is an integer in the range from 2001 to 2036.
{ first | second | third | fourth | fifth | last }	Specifies the first, second, third, fourth, fifth, or last workday in a month when the daylight saving time starts or ends.	-

Default Value

By default, the daylight saving time is not set.

View

Global configuration view

Usage Guidelines

You can use this command to set the daylight saving time rule in the local time zone. The configuration takes effect between years 2001 and 2100. After a rule is configured, the daylight saving time will take effect on the switch based on the configured rule.

Example

Configure the daylight saving time to start at 1:0 on 7/15/2019 and end at 23:59 on 8/31/2019.

```
switch(config)#clock summer-time BJ date 1:0 2019/7/15 23:59 2019/8/31
switch(config)#quit
switch#show clock
  System Running Time : 0 hours,30 minutes,46 seconds
  Clock                       : 2000-04-06 10:16:42
  Time Zone                   : UTC +00:00
  Summer Time                 :
          Name                : BJ
          Repeat mode    : date
          Start year     : 2019
          End year       : 2019
          Start time     : 7/15/2019 01:00
          End time       : 8/31/2019 23:59
switch#
```

Cancel the configuration of daylight saving time.

```
switch(config)#no clock summer-time
switch(config)#quit
switch#show clock
  System Running Time : 0 hours,31 minutes,10 seconds
  Clock                       : 2000-04-06 10:17:06 AM
```

```
  Time Zone                : UTC +00:00
switch#
```

1.2.6 clock timezone

Function

The **clock timezone** command sets the local time zone.
The **no clock timezone** command restores the local time zone to the Universal Time Coordinated (UTC) time zone.

Format

- **clock timezone** *time-zone-name* { **add** | **minus** } *offset*
- **no clock timezone**

Parameters

Parameters	Description	Value
time-zone-name	Specifies the name of the time zone.	The value is a string of 1 to 10 characters.
add	Specifies the incremental offset against the UTC. That is, the time zone specified by *time-zone-name* can be obtained by adding *offset* to the default UTC.	-
minus	Specifies the decremental offset against the UTC. That is, the time zone specified by *time-zone-name* can be obtained by deducting *offset* from the default UTC.	-
offset	Specifies the time difference with the UTC.	The value is in the format of *HH:MM*, in which H indicates hour in the range from 0 to 12, and M indicates minute in the range from 0 to 59.

Default Value

By default, the time zone setting is UTC +00:00.

View

Privileged user view

Usage Guidelines

None

Example

Set the local time zone name to Delaware.

```
switch#clock timezone Delaware add 8:0
  Finishing writing the configuration file.

switch#show clock
  clock : 1/3/2100 7:36:44 AM
  Time Zone:Delaware +08:00
  System running time : 1 hours,0 minutes,46 seconds
switch#
```

1.2.7 clear configuration

Function

The **clear configuration** command clears all the configuration of an interface.

Format

- **clear configuration**

Parameters

None

Default Value

None

View

Interface configuration view, Interface group configuration view

Usage Guidelines

None

Example

Clear all the configuration of an interface.

```
switch(config-100ge1/0/52)#clear configuration
  WARNING:All configuration of the interface will be cleared, and its state will be shutdown.Continue?(y/n) [y]y
switch(config-100ge1/0/52)#
```

1.2.8 cls

Function

The **cls** command clears information displayed on the current CLI.

Format

- **cls**

Parameters

None

Default Value

None

View

All configuration views except the common user view

Usage Guidelines

If too much information is displayed on CLI and affects operations on the system or you no longer need the displayed information, run this command to clear the information.

Example

Clear the information displayed on the CLI.

```
switch#cls
switch#
```

1.2.9 configure

Function

The **configure** command is used to switch from the privileged user view to the global configuration view.

Format

- **configure**

Parameters

None

Default Value

None

View

Privileged user view

Usage Guidelines

In the privileged user view, you can check all running status and statistical information on the switch, and manages files and the system.
In the global configuration view, you can configure global Parameters of the switch in addition to configuration privileges in the privileged user view.

Example

Switch from the privileged user view to the global configuration view.

```
switch#configure
switch(config)#
```

1.2.10 disable

Function

The **disable** command returns to the global configuration view from the privileged user view.

Format

The **disable** command returns to the global configuration view from the privileged user view.
The **disable** *privilege-value* command lowers the privilege of the current user to 0-15. The default user privilege is 15.

Format

- **disable**
- **disable** *privilege-value*

Parameters

Parameters	Description	Value
privilege-value	Specifies a user privilege level.	The value is an integer in the range from 0 to 15.

Default Value

None

View

Privileged user view

Usage Guidelines

None

Example

Return to the global configuration view from the privileged user view.

```
switch#disable
switch#
```

1.2.11 enable

Function

The **enable** command switches from the common user view to the privilege view.
The **enable** *privilege-value* command elevates the privilege of the current user to 0-15. The default user privilege is 15.

Format

- **enable**
- **enable** *privilege-value*

Parameters

Parameters	Description	Value
privilege-value	Specifies a user privilege level.	The value is an integer in the range from 0 to 15.

Default Value

None

View

Common user view

Usage Guidelines

None

Example

Switch from the common user view to the privilege view.

```
switch#enable
switch#
```

1.2.12 enable password

Function

The **enable password** command sets the global local secondary authentication password for users of level 0-15.

The **no enable password** command deletes the global local secondary authentication password for users of level 0-15.

Format

- **enable password level** *level-value* { **cipher** | **plain** } *password*
- **enable password** { **cipher** | **plain** } *password*
- **no enable** *level-value* **password**
- **no enable password**

Parameters

Parameters	Description	Value
level-value	Specifies a privilege level.	It is an integer, and the value ranges from 0 to 15.
{cipher|plain}	Displays a password in cipher text or plain text.	-
password	Specifies a password.	The value is a character string.

Default Value

None

View

Global configuration view

Usage Guidelines

If you do not specify a privilege level in the command, the command configures or deletes the local secondary authentication password for users of level 15.

Example

```
switch(config)#enable password cipher password testkey
switch(config)#
```

1.2.13 end

Function

The **end** command returns to the privilege view from the current configuration view.

Format

- **end**

Parameters

None

Default Value

None

View

All configuration views

Usage Guidelines

You can use this command to return to the privilege view directly from any configuration view.

Example

Return to the privileged user view.

```
switch(config)#end
switch#
```

1.2.14exit

Function

The **exit** command returns to the previous configuration view from the current configuration view. If you run this command in the common user view or privilege view, the login interface will be displayed or the connection with the switch will be terminated.

Format

- **exit**

Parameters

None

Default Value

None

View

All configuration views

Usage Guidelines

You can use this command to exit from the current configuration view and return to the previous lower-level configuration view.

The **end** and **exit** commands differ in that the **end** command returns to the privileged user view regardless of the current view, whereas the **exit** command returns to the previous configuration view.

By running the **exit** command, you can return to the lower-level command mode from a higher-level command mode. You can also switch between command modes of the same level. In addition, you can press **Ctrl**+**Z** or run the **end** command to return to the privileged user view from two higher-level views.

Example

Return to the previous lower-level configuration view.

```
switch(config-vlan10)#exit
switch(config)#
```

1.2.15 help

Function

The **help** command displays system help information.

Format

- **help**

Parameters

None

Default Value

None

View

All configuration views

Usage Guidelines

The switch provides convenient online help. The **help** command displays information about the entire online help system. You can type in a question mark (?) anytime, anywhere to obtain all or part of help information.
If no related online help information is available, no information will be displayed. You need to return to the previous state, until online help information is displayed after you type in .

Example

Display online help information.

```
switch#help
When you need help,anytime at the command line please press '?'.
If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1.Full help is available when you are ready to enter a command
argument (e.g. 'show ?') and describes each possible argument.

2.Partial help is provided when an abbreviated argument is entered
and you want to know what arguments match the input (e.g. 'show me?'.)
switch#
```

1.2.16hostname

Function

The **hostname** command sets the host name of the switch.
The **no hostname** command restores the default host name of the switch.

Format

- **hostname** *hostname*
- **no hostname**

Parameters

Parameters	Description	Value
hostname	Specifies a host name for the switch.	The value is a string of 1 to 128 characters.

Default Value

The default device name is switch.

View

Global configuration view

Usage Guidelines

Changing the host name of the switch will change the prompt displayed on the CLI. For example, if the host name of the switch is set to switch, the prompt in the user view will be switch.

Example

Set the host name of the switch to Switch.

```
switch(config)#hostname Switch
switch(config)#
```

1.2.17list

Function

The **list** command displays all the commands that can be used in the current configuration view.

Format

- **list** [*keyword*]

Parameters

Parameters	Description	Value
[keyword]	Specifies a command keyword.	The value is a character string.

Default Value

None

View

All configuration views

Usage Guidelines

This command is similar to the **dir** command in the MS-DOS system and the **ls** command in the UNIX system. The advantage of this command is that you need not remember all commands. If you forget a command, use this command to find the desired command.

Example

Display all the commands available in the privileged user configuration view.

```
switch#list
  capture cpupkt interface (10gigaethernet|100gigaethernet) <1-1>/<0-2>/<1-52> time <1-1800>
  capture cpupkt interface eth-trunk <1-124> time <1-3600>
  capture cpupkt interface ethernet <0-0>/<0-0>/<0-0> time <1-3600>
  capture cpupkt interface iss-trunk <1-2> time <1-3600>
  cd
  cd DIR
  clear abnormal-log
  clock set <0-23>:<0-59>:<0-59> <1-31> <1-12> <2001-2036>
  clock set <0-23>:<0-59>:<0-59> <2001-2036> <1-12> <1-31>
  clock summer-time NAME date <0-23>:<0-59> <1-31> <1-12> <2001-2036> <0-23>:<0-59> <1-31> <1-12>
<2001-2036>
  clock summer-time NAME date <0-23>:<0-59> <2001-2036>/<1-12>/<1-31> <0-23>:<0-59>
<2001-2036>/<1-12>/<1-31>
  clock summer-time NAME recurring (first|second|third|fourth|fifth|last)
(monday|tuesday|wednesday|thursday|friday|saturday|sunday)
 (january|february|march|april|may|june|july|august|september|october|november|december) <0-23>:<0-59>
(first|second|third|fourth|fi
fth|last) (monday|wednesday|tuesday|thursday|friday|saturday|sunday)
(january|february|march|april|may|june|july|august|september|oc
tober|november|december) <0-23>:<0-59>
  clock timezone NAME (add|minus) <0-12>:<0-59>
  cls
  compare configuration <1-65535> <1-65535>
  compare configuration startup-config
  configure
  copy SRCFILE DESTFILE
```

--More--

1.2.18 management acl|management acl6

Function

The **management acl|management acl6** command enables or configures the ACL.
The **no management acl|no management acl6** command cancels the configuration.

Format

- **management acl** { **enable** | **disable** }
- **management acl** *ipv4-address*
- **management acl** *ipv4-address/M*
- **management acl** *ipv4-address/M* { **telnet** | **snmp** | **ssh** | **ftp** | **all** }
- **management acl6** *ipv6-address/M*
- **management acl6** *ipv6-address/M* { **telnet** | **snmp** | **ssh** | **all** }
- **no management acl** *ipv4-address/M*
- **no management acl6** *ipv6-address/M*

Parameters

Parameters	Description	Value
enable	Enables the ACL.	-
disable	Disables the ACL.	-
ipv4-address	Specifies an IPv4 address or a network segment address visited by a user.	The value is in dotted decimal notation. For example, an IPv4 address is in the A.B.C.D format.
ipv6-address	Specifies an IPv6 address or network segment that the user host can access.	An IPv6 address is in the X:X::X:X format.
M	Specifies the mask length.	The value is an integer. For an IPv4 address, the mask length ranges from 1 to 32. For an IPv6 address, the mask length is 128.
telnet|web|snmp|ssh|ftp|all	Configures an ACL for a Telnet, web, SNMP, SSH, or FTP user, or all of these users.	-

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Enable the ACL function.

```
switch(config)#management acl enable
switch(config)#
```

Enable the user with IP address 10.2.3.1 and mask 255.255.255.255 to log into the switch using Telnet.

```
switch(config)#management acl 10.2.3.1 255.255.255.255 telnet
switch(config)#
```

1.2.19 password

Function

The **password** command changes the password of the current user.

Format

- **password** *password*
- **password** *password* **simple**

Parameters

Parameters	Description	Value
password	Specifies the new password of the current user.	The value is a string of 1 to 64 characters.
simple	Specifies that the new password is encrypted using a reversible algorithm. Otherwise, the new password is encrypted using the MD algorithm.	-

Default Value

The system has a default user with the administrator privilege. The user name is **admin** and password is **12345**.

View

Common user view, privileged user view and global configuration view

Usage Guidelines

The switch supports both reversible and irreversible encryption algorithms for the user password because some authentication methods (such as dot1x) require plaintext passwords of users. Irreversible encryption cannot be used in this scenario.

Example

Change the password of the current user to **fs0001**.

```
switch(config)#password fs0001
switch(config)#
```

1.2.20 ping

Function

The **ping** command tests the connectivity of an IP network.

Format

- **ping** *ipv4-address string*
- **ping** *ipv4-addres* **-t**
- **ping** *ipv4-address* **{ -n | -q | -f | -h | -l | -w | -tos | -m | -dscp | -8021p}** *VALUE1*

Parameters

Parameters	Description	Value
ipv4-address	Specifies an IPv4 address.	The value is in dotted decimal notation.
string	Detailed Parameters depend on the help prompt of a switch.	-n | -t | -q | -f | -h | -l | -w | -tos | -m | -dscp | -8021p | -s

Default Value

None

View

Privileged user view and global configuration view

Usage Guidelines

If an IP network fails, you can use this command to locate the failure point.
In a ping test, a switch sends ICMP Echo Request packets to the destination host. If the network connection with the destination is normal,
the destination responds with ICMP Echo Reply packets after receiving the ICMP Echo Request packets.
The **ping** command can be used to determine whether a network connection failure occurs or to evaluate the quality of network lines. The command output information includes the following:
Response of destination host to each Echo Request packet. If a switch does not receive an Echo Reply packet, it displays "Request time out." If a switch receives an Echo Reply packet, it displays the number of bytes, response time, Time-to-Live (TTL) value, and sequence number of the packet.
Final statistics, including the number of packets sent, number of reply packets received, percentage of packets for which no reply is received, as well as the minimum, maximum, and average of response time.

Example

Test whether the IP address 10.18.10.8 is reachable.

```
switch#ping 10.18.10.8 -t
PING 10.18.10.8: 56 data bytes
Reply from 10.18.10.8: bytes=64 time=0ms TTL=128 icmp_seq=0
Reply from 10.18.10.8: bytes=64 time=0ms TTL=128 icmp_seq=1
Reply from 10.18.10.8: bytes=64 time=0ms TTL=128 icmp_seq=2
Reply from 10.18.10.8: bytes=64 time=0ms TTL=128 icmp_seq=3
Reply from 10.18.10.8: bytes=64 time=0ms TTL=128 icmp_seq=4
PING Statistic for 10.18.10.8
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)    min/avg/max = 0/0/0
switch#
```

1.2.21ping6

Function

The **ping6** command checks the reachability of a host. After sending an ICMPv6 request packet, the switch waits for the response from the destination host.
The **ping6 -t** command checks network connectivity and pings the designated host until the operation is manually stopped.

Format

- **ping6** *ipv6-addres*
- **ping6** *ipv6-addres* **-t**
- **ping6** *ipv6-addres* **{ -n | -l | -w |-m | -dscp | -8021p }** *VALUE*

Parameters

Parameters	Description	Value
ipv6-address	Specifies the destination IPv6 address.	A 128-bit IPv6 address is divided into 8 groups, with 16 bits in each group. Each group is expressed by four hexadecimal digits (0-9 and A-F), and two groups are separated with a colon (:). Each X represents a group of hexadecimal digits.
string	Detailed Parameters depend on the help prompt of a switch.	-n | -t | -l | -w |-m | -dscp | -8021p | -s

Default Value

None

View

Privileged user view and global configuration view

Usage Guidelines

None

Example

Ping whether the network of the interface with IPv6 address 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A is connected.

```
switch#ping6 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A
ping statistics for 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A :
        Packets:Send = 7,    Received = 0 , Lost = 7 (100% loss),
Approximate round trip times in milli-seconds:
        Minimum = 0ms,    Maximum = 0ms , Average = 0ms
switch#
```

1.2.22 quit

Function

The **quit** command returns to the previous configuration view from the current configuration view. If you run this command in the common user view or privilege view, the login interface will be displayed or the connection with the switch will be terminated.

Format

- **quit**

Parameters

None

Default Value

None

View

All configuration views

Usage Guidelines

By running the **quit** command, you can return to the lower-level command mode from a higher-level command mode. You can also switch between command modes of the same level. You can also press **Ctrl**+**Z** to directly return to the privileged user configuration mode from a higher-level mode. This command provides the same function as the **exit** command.

Example

Return to the previous lower-level configuration view.

```
switch(config-vlan10)#quit
switch(config)#
```

1.2.23 reboot

Function

The **reboot** command reboots the switch.
The **reboot member** command restarts a switch in a stack system.

Format

- **reboot**

Parameters

None

Default Value

None

View

All configuration views

Usage Guidelines

This command provides the same function as a cold restart. Using this command, you can reboot the switch remotely, without the need to go to the equipment room. Do not use this command unless necessary, because it will cause a temporary interruption of the network. In addition, you are advised to determine whether to save the configuration file before the reboot.

Example

Restart a switch.

```
switch#reboot
  WARNING:System will reboot! Continue?(y/n) [y]y
  System now is rebooting,please wait.
switch#
```

1.2.24 reboot {at|in}

Function

The **reboot at** command reboots the switch at specified time.
The **reboot in** command reboots the switch after a specified delay.

Format

- **reboot at** *time1*
- **reboot at** *time2*
- **reboot in** *time*

Parameters

Parameters	Description	Value
time1	Specifies the time to reboot the switch.	The value is an integer, in the format of 0-23:0-59.
time2	Specifies the time to reboot the switch.	The value is an integer, in the format of 1-31:1-12.
at	Reboots the switch at the specified time.	-
in	Reboots the switch after a specified delay.	-

Default Value

None

View

Privileged user view and global configuration view

Usage Guidelines

None

Example

Reboot the switch at 23:23.

```
switch(config)#reboot at 23:23
  WARNING:System will reboot after a specified delay! Continue?(y/n) [y]y
  System will rebooting at 2017-08-17 14:45:57 (after 23 hours 23 minutes),please wait.
```

1.2.25 reboot cancel

Function

The **reboot cancel** command cancels scheduled reboot of the switch.

Format

- **reboot cancel**

Parameters

None

Default Value

None

View

Privileged user view and global configuration view

Usage Guidelines

None

Example

Cancel scheduled reboot of the switch.

```
switch(config)#reboot in 23:23
  WARNING:System will reboot after a specified delay! Continue?(y/n) [y]y
  System will rebooting at 2019-08-17 14:45:57 (after 23 hours 23 minutes),please wait.


switch(config)#reboot cancel
  WARNING:System will cancel reboot! Continue?(y/n) [y]y
  System now canceled reboot.
```

1.2.26 reset recycle

Function

The **reset recycle** resets the recycle bin.

Format

- **reset recycle**

Parameters

None

Default Value

None

View

Privileged user view and global configuration view

Usage Guidelines

None

Example

Reset the recycle bin.

```
switch(config)#reset recycle
switch(config)#
```

1.2.27 send message

Function

The **send message** command sends messages from one user terminal to another user terminal.

Format

- **send message** *data*
- **send message**

Parameters

Parameters	Description	Value
data	Specifies the content of the message to be sent.	The value is a character string.

Default Value

None

View

Privileged user view

Usage Guidelines

You can use this command to send a message from the current user terminal to all the other user terminals that have logged into the system. When you run **send message** *data*, a message will be send immediately after you press **Enter**. If you run **send message**, press **Enter**, and then enter the message, you must press **Ctrl+Z** as required to send the message.

Example

Send a message "Hello" from the current user terminal to all the other user terminals that have logged into the system.

```
switch#send message Hello
switch#
```

1.2.28 show clock

Function

The **show clock** command displays the current time of a system and how long the system has been running.

Format

- **show clock**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, and VLAN configuration view

Usage Guidelines

You can use this command to check whether the current date and time on the switch are consistent with those in logs. Moreover, you can check how long the switch has been running.

Example

Display the current date and time on the switch.

```
switch#show clock
  System Running Time : 1 hours,37 minutes,54 seconds
  Clock                    : 2019-09-24 15:39:30 Tue
  Time Zone                : UTC +00:00
switch#
```

1.2.29 show command-privilege

Function

The **show command-privilege config** command displays the priority configuration of a command.
The **show command-privilege verbose** command displays the detailed priority of a command.

Format

- **show command-privilege config**
- **show command-privilege verbose**

Parameters

None

Default Value

None

View

Privileged user view

Usage Guidelines

None

Example

Display the priority configuration of a command.

```
switch#show command-privilege config
switch#
```

1.2.30 show history

Function

The **show history** command displays the historical commands used by the user.

Format

- **show history**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

You can use this command to view the recently used commands.

Example

Display historical commands that have been used recently.

```
switch#show history
  configure
  cfm
  list
  md name testmd level 1
  ma name testma vlan 1
  q
  y1731
  meg vlan 1 level 1 icc feisu1 umc feisu2
  q
  list diffserv
  list netflow
  list drop
  list drop-profile
  q
  clock summer-time BJ date 1:0 2019/7/15 23:59 2019/8/31
  show clock
  no clock summer-time
  show clock
  list
  show cpu statistic
switch#
```

1.2.31show login-type count

Function

The **show login-type count** command displays the terminal numbers of different login modes.

Format

- **show login-type count**

Parameters

None

Default Value

None

View

Privileged user view and global configuration view

Usage Guidelines

None

Example

View the number of terminals using different login modes.

```
switch#show login-type count
  LoginType              Count
  Console                1
  Telnet                  1
  Ssh                    3
  Http                    3
switch#
```

1.2.32 show management acl

Function

The **show management acl** command displays the ACL configuration.

Format

- **show management acl**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Show the configuration of the ACL.

```
switch(config)#show management acl
  Management Acl State: Disable
switch(config)#
```

1.2.33 show module version

Function

The **show module version** command displays the versions of protocol modules.

Format

- **show module version**

Parameters

None

Default Value

None

View

Privileged user view

Usage Guidelines

None

Example

Display the versions of protocol modules.

```
switch#show module version
Module                          : Version
cli                            : CLI_VX2.12.02.00
snmp                            : SNMP_VX2.11.00.00
stp                            : MSTP_VB3.01.00.00
flink                          : RLINK_VB3.00.02.00
mlink                           : MLINK_VB3.00.01.00
flush                          : FLUSH_VB3.00.01.00
vlan-mapping                    : VLANMAPPING_VB3.00.02.00
qinq                           : QINQ_VB3.00.02.00
```

```
port-isolate                    : PORTISOLATE_VB3.00.08.00
bfd                              : BFD_VX2.10.00.00
udld                             : UDLD_VB3.00.05.00
lldp                            : LLDP_VB3.00.04.00
aaa                              : AAA_VB3.00.00.00
mvrp                             :
vtp                             : VTP_VB3.00.00.00
switch#
```

1.2.34 show privilege

Function

The **show privilege** command shows the user level of the current login user.

Format

- **show privilege**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, and interface group configuration view

Usage Guidelines

- The N-series switch supports the following privileges:
- Administrators: Specify the administration level, corresponding to level 15.
- Operators: Specify the operation level, corresponding to level 11.
- Users: Specify the user level, corresponding to level 7.
- Guests: Specify the visit level, corresponding to level 3.

Example

Show the user level of the current login user.

```
switch#show privilege
  %Current privilege level is 3.
switch#
```

1.2.35 show reboot

Function

The **show reboot** command displays the reboot management configuration.

Format

- **show reboot**

Parameters

None

Default Value

None

View

Privileged user view and global configuration view

Usage Guidelines

None

Example

Display the reboot management configuration.

```
switch#show reboot
  System will reboot at 9/15/2019 18:00:23
switch#
```

1.2.36 show system

Function

The **show system** command displays the default MAC address of the switch and the currently used MAC address.

Format

- **show system**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Show the default MAC address and currently used MAC address on the switch.

```
switch#show system
```

```
  System device code   : G5F8200T00B19062102
  Default mac-address : 00:00:02:fb:79:af
  Current mac-address : 00:00:02:fb:79:af
  System boot image    : Main
  System boot config   : Main
switch#
```

1.2.37 show user config

Function

The **show user config** command displays the attributes of an existing local user.

Format

- **show user config**
- **show user config** *verbose*

Parameters

None

Default Value

None

View

Privileged user view and global configuration view

Usage Guidelines

None

Example

Show the attributes of the local user 123.

```
switch#show user config verbose
  User name                          : admin
  User group                         :  administrators
  Password type                      :  cipher
  Password complexity                :  1
  Authtication max fail count        :  3
  User reauthtication interval       :  0(minutes)
  User online count                  :  5
switch#
```

1.2.38 show version

Function

The **show version** command displays information such as the current software version and hardware version.

Format

- **show version**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Show the current version information of the system.

```
switch#show version
  FS Platform
  Copyright (c) 2000-2019, Feisu Technologies Co., Ltd.
  V310R230
  Feisu Switch
  System Uptime is 0 days 1 hours 13 minutes 4 seconds

  Hardware Version : 1.02
  BIOS Version     : 1.16
  FPGA Version     : 1.04
  Serial Number    :
  System Memory    : 512916K
  Total Flash      : 64MB
  Free Flash       : 13.0MB
switch#
```

1.2.39 temporary-password

Function

The **temporary-password** command enables or disables the temporary password.

Format

- **temporary-password** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the temporary password function.	-
disable	Disables the temporary password function.	-

Default Value

Enable

View

Global configuration view

Usage Guidelines

None

Example

Disable the temporary password.

```
switch(config)#temporary-password disable
switch(config)#
```

1.2.40 trace|trace6

Function

The **trace** command tests the connectivity of an IPv4 network.
The **trace6** command tests the connectivity of an IPv6 network.

Format

- **trace** *ipv4-address string*
- **trace6** *ipv6-address string*

Parameters

Parameters	Description	Value
ipv4-address	Specifies the IP address of the host to which the network connectivity needs to be tested.	The value is in dotted decimal notation.
ipv6-address	Specifies an IPv6 address.	A 128-bit IPv6 address is divided into 8 groups, with 16 bits in each group. Each group is expressed by four hexadecimal digits (0-9 and A-F), and two groups are separated with a colon (:). Each X represents a group of hexadecimal digits.
string	Detailed Parameters depend on the help prompt of a switch.	-n|-r|-q|-f|-system-time|-l|-w|-m|-h|-tos|-dscp|-8021p|-nexthop|-s

Default Value

None

View

Global configuration view

Usage Guidelines

If an IP network fails, you can use this command to locate the failure point.

Example

Test whether the IPv4 address 192.168.1.118 is reachable.

```
switch#traceroute 192.168.1.118
 Tracing route to 192.168.1.118 over a maximum of 16 hops.
  1          16 ms          <16 ms          <16 ms          192.168.1.118

 Trace complete.

switch#
```

1.2.41user fail-count

Function

The **user fail-count** command sets the maximum number of continuous login failures allowed for a specified user.

Format

- **user fail-count** *fail-count-time*
- **username** *user-name* **fail-count** *fail-count-time*

Parameters

Parameters	Description	Value
user-name	Specifies a user name. The specified user must have been created.	The value is a character string.
fail-count-time	Specifies the maximum number of login failures.	The value is an integer ranging from 1 to 10.

Default Value

By default, a maximum of 3 login failures are allowed for a user.

View

Global configuration view

Usage Guidelines

Before using this command, run the **user reauth-interval** command first to set the user reauthentication interval; otherwise this command will not take effect.

Example

Set the maximum number of login failures of a user to 5.

```
switch(config)#user fail-count 5
switch(config)#
```

1.2.42 show

Function

The **show** command outputs all configuration of the module node under the current protocol.

Format

- **show**

Parameters

None

Default Value

None

View

All configuration views except the common user view

Usage Guidelines

You can obtain configuration information of the current node after you enter each protocol node in the configuration view using this command.

Example

Output all configuration of the current node.

```
switch(config)#show
  %Command incomplete.
switch(config)#aaa
switch(config-aaa)#show
aaa
 radius-server test ip-address 1.1.1.1 key 123
switch(config-aaa)#
```

1.2.43 user same-name-pwd

Function

The **user same-name-pwd** command configures whether to permit or deny access from a login user with identical user name and password.

Format

- **user same-name-pwd** { **permit** | **deny** }

Parameters

Parameters	Description	Value
permit	Permits access from a login user with identical user name and password.	-
deny	Denies access from a login user with identical user name and password.	-

Default Value

Deny

View

Global configuration view

Usage Guidelines

None

Example

Permit access from a login user with identical user name and password.

```
switch(config)#user same-name-pwd permit
switch(config)#
```

1.2.44 user reauth-interval

Function

The **user reauth-interval** command sets the reauthentication interval of a user when the number of authentication failures reaches the upper limit.

Format

- **user reauth-interval** *reauth-interval-time*
- **username** *user-name* **reauth-interval** *reauth-interval-time*

Parameters

Parameters	Description	Value
user-name	Specifies a user name. The specified user must have been created.	
reauth-interval-time	Specifies the reauthentication interval of users.	The value is an integer in the range from 0 to 65535, in minutes.

Default Value

By default, the reauthentication interval is 0.

View

Global configuration view

Usage Guidelines

When the number of continuous authentication failures reaches the upper limit, you need to wait for reauthentication after the reauthentication interval ends.

Example

Set the reauthentication interval of the user feisu to 20 minutes.

```
switch(config)#username feisu reauth-interval 20
switch(config)#
```

1.2.45 username

Function

The **username** command changes the privilege group of a specified user.
The **no username** command deletes a specified user.

Format

- **username** *user-name* **group** { **administrators** | **operators** | **users** | **guests** }

- **no username** *user-name*

Parameters

Parameters	Description	Value
user-name	Specifies the name of the user for which you want to change the privilege group.	The value is a character string.
administrators	Specifies the privilege of the administrator level.	-
operators	Specifies the privilege of the operator level.	-
users	Specifies the privilege of the user level.	-
guests	Specifies the privilege of the guest level.	-

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to change the privilege group of the user. Ensure that the specified user exists in the system. To run this command, you must have the administrator privilege.

Users on the switch are divided into four privilege groups, listed in descending order of level:

- The administrators group has the highest level and can run any commands. Key commands or important operations that have great impact on the switch can only be performed by users in this privilege group. Such operations include user management, FTP operation, clearing historical records, reducing the number of terminals, upgrading image and configuration files, and enabling or disabling the FTP/Telnet function.
- The operators group has a lower level than the administrators group, and can run all commands except those related to key operations requiring the administrator privilege.
- The users group has a lower level than the operators group, and can run all commands except upgrade, tftp, sgm commands.
- The guests group has the lowest level and can run only information display commands and a few configuration commands, such as **ping** commands. Notice that the guests group cannot view important information such as output information of **show logging**, **show running-config**, **show snmp config**, **show startup-config**, and **show user config** commands.

Example

Create a user account, with the user name **test**, group **users**.

```
switch(config)#username test group users
switch(config)#
```

1.2.46 username domain

Function

The **username domain** command configures different domains to manage user login rights and specifies a user to join one or all domains.
The **no username domain** command configures different domains to manage user login rights and specifies a user to exit from one or all domains.

Format

- **username** *user-name* **domain** { **telnet** | **ssh** | **console** }
- **username** *user-name* **domain all**
- **no username** *user-name* **domain** { **telnet** | **ssh** | **console** }
- **no username** *user-name* **domain all**

Parameters

Parameters	Description	Value
user-name	Specifies the name of the user that you want to add to or remove from the domain.	The value is a character string.
telnet	Supports Telnet login.	-
ssh	Supports Secure Shell (SSH) login.	-
console	Supports serial port login.	-
all	Access device by telnet,ssh and console	-

Default Value

None

View

Global configuration view

Usage Guidelines

A new user has only the rights to log into the serial port. The administrator has the rights to log into the serial port through Telnet, FTP, and SSH.

Example

Add the user test to the telnet domain.

```
switch(config)#username test domain telnet
switch(config)#
```

1.2.47 username group password

Function

The **username group password** command creates a user account for logging into the switch.

Format

- **username** *user-name* **password** *password*
- **username** *user-name* **password** *password* **simple**
- **username** *user-name* **group** { **administrators** | **operators** | **users** | **guests** } **password** *password*
- **username** *user-name* **group** { **administrators** | **operators** | **users** | **guests** } **password** *password* **simple**

Parameters

Parameters	Description	Value
user-name	Specifies the user name of the account.	The value is a character string.
administrators	Specifies the privilege of the administrator level.	-
operators	Specifies the privilege of the operator level.	-
users	Specifies the privilege of the user level.	-
guests	Specifies the privilege of the guest level.	-
simple	Specifies that the user password is encrypted using a reversible encryption algorithm.	-
password	Specifies the password of the account.	The value is a string of 1 to 64 characters.

Default Value

None

View

Global configuration view

Usage Guidelines

If you do not specify a privilege group when using this command to create a user, the user is added to the default privilege group **operators**. When creating a dot1x user, you can only set a password by specifying the **simple** keyword. If you want to delete a user but specify a nonexistent user, an operation failure message will be displayed.
To run this command, you must have the administrator privilege.
Users on the switch are divided into four privilege groups, listed in the descending order of level:

- The administrators group is the highest level and can configure users. Users of other levels do not have the user configuration privilege. The corresponding level is 15.
- The operators group can use all commands except the user configuration commands. This user level can be used for device configuration and management. The corresponding level is 11.
- The users group cannot use ring configuration commands. The corresponding level is 7.

- The guests group can only be used for device maintenance and cannot use configuration commands. The corresponding level is 3.

Example

Create a user account, with the user name test, privilege group users, and password test.

```
switch(config)#username test group users password test
switch(config)#
```

1.2.48 username online-count

Function

The **username online-count** command sets the maximum number of concurrent online users allowed on the switch.

Format

- **username** *user-name* **online-count** *online-count-num*

Parameters

Parameters	Description	Value
user-name	Specifies a user name. The specified user must have been created.	The value is a character string.
online-count-num	Specifies the maximum number of online users.	The value is an integer in the range from 1 to 64.

Default Value

By default, a maximum of 5 users can stay online.

Command Mode

Global configuration view

Usage Guidelines

Before running this command, use the **username** command to create the specified user.

Example

Set the maximum number of online users to 8.

```
switch(config)#username feisu online-count 8
switch(config)#
```

1.2.49 user pwd-complex

Function

The **user pwd-complex** command sets the user password complexity.

Format

- **user pwd-complex** *pwd-complex*

Parameters

Parameters	Description	Value
pwd-complex	Specifies the password complexity.	The value is an integer ranging from 1 to 4.

Default Value

1

View

Global configuration view

Usage Guidelines

The **user pwd-complex** command sets the password complexity for all users in the system.

Example

Set the password complexity of all users to 1.

```
switch(config)#user pwd-complex 1
switch(config)#
```

1.2.50 user pwd-length

Function

The **user pwd-length** command sets the password length for a specified user or all users in the system.

Format

- **user pwd-length** *pwd-length*

Parameters

Parameters	Description	Value
pwd-length	Specifies the password length.	The value is an integer ranging from 1 to 64.

Default Value

1

View

Global configuration view

Usage Guidelines

If you do not set the *word* Parameters (user name), the command sets the password length for all users in the system.

Example

Set the password length to 32 characters for all users.

```
switch(config)#user pwd-length 32
switch(config)#
```

1.2.51unlock-command vty

Function

The **unlock-command vty** command unlocks a command.

Format

- **unlock-command vty** *vty-value*

Parameters

Parameters	Description	Value
vty-value	Specifies a command node number.	The value is an integer in the range from 1 to 32.

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Unlock a command.

```
switch(config)#unlock-command vty 1
switch(config)#
```

1.2.52 who

Function

The **who** command displays information about the users who have logged in and are configuring the switch.

Format

- **Who**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

You can use this command to check which users are configuring the switch. The user name with an asterisk (*) is the one you are using.

Example

View the information about users who have logged in and are configuring the switch.

1.3 User Terminal Configuration Commands

1.3.1 case-sensitive

Function

The **case-sensitive** command configures the CLI terminal to be case sensitive or case insensitive.

Format

- **case-sensitive** { **enable** | **disable** }

Parameters

Parameter	Description	Value
enable	Configures the terminal to be case sensitive.	-
disable	Configures the terminal to be case insensitive.	-

Default Value

enable

View

Global configuration view

Usage Guidelines

None

Example

Configure the CLI terminal to be case insensitive.

```
switch(config)#case-sensitive disable
switch(config)#
```

Related Commands

None

1.3.2 color

Function

The **color** command sets the background color of the terminal. The system supports the following colors: gray, red, green, yellow, blue, purple, water, and white.
The **no color** command cancels the background color setting of a terminal.

Format

- **color** { **gray** | **red** | **green** | **yellow** | **blue** | **purple** | **water** | **white**}
- **no color**

Parameters

None

Default Value

None

View

Line configuration view

Usage Guidelines

None

Example

Set the background color of a terminal to blue.

```
switch(config)#line vty 1
switch(config-line)#color blue
```

Related Commands

None

1.3.3 monitor

Function

The **monitor** command enables the CLI terminal to receive debugging information.
The **no monitor** command disables the CLI terminal from receiving debugging information.

Format

- **monitor**
- **no monitor**

Parameters

None

Default Value

By default, terminals that log in through the serial port can receive debugging information, and those that log in through Telnet cannot receive debugging information.

View

Line configuration view

Usage Guidelines

This command determines whether the virtual terminal can receive debugging information. If you run monitor, the virtual terminal can receive debugging information. If you run no monitor, the virtual terminal cannot receive debugging information. This command can be used in the terminal configuration view.

Example

Enable the CLI terminal to receive debugging information.

```
switch(config)#line vty 1
```

```
switch(config-line)#monitor
```

Related Commands

None

1.3.4 language

Function

The **language** command configures the language of help information displayed on the user terminal.

Format

language { **chinese** | **english** }

Parameters

Parameter	Description	Value
chinese	Displays help information in Chinese.	-
english	Displays help information in English.	-

Default Value

None

View

Line configuration view

Usage Guidelines

None

Example

Set the language of help information displayed on the switch to English.

```
switch(config-line)#language english
switch(config-line)#
```

Related Commands

None

1.3.5 length

Function

The **length** command sets the number of lines that can be displayed on the CLI terminal.
The **no length** command restores the number of lines that can be displayed on the CLI terminal to the default value.

Format

- **length** *length*
- **no length**

Parameters

Parameter	Description	Value
length	Specifies the number of lines that can be displayed on the CLI terminal.	The value is 0 or an integer ranging from 0 to 512.

Default Value

By default, 25 lines of information can be displayed on the CLI terminal.

View

Line configuration view

Usage Guidelines

You can use this command to set the number of lines displayed on a screen when using the CLI. If the length is set to 0, the multi-screen display function is disabled.

Example

Set the number of lines that can be displayed on the CLI terminal to 30.

```
switch(config-line)#length 30
switch(config-line)#
```

Related Commands

None

1.3.6 line console

Function

The **line console** command displays the console terminal configuration view.

Format

- **line console**
- **line console** *number*

Parameters

Parameter	Description	Value
number	Specifies the number of the console terminal to be configured.	The value is an integer ranging from 1 to 1.

Default Value

None

View

Global configuration view, line configuration view

Usage Guidelines

Using this command, you can enter the console terminal configuration view to set attributes of the terminal.

Example

Enter the console terminal configuration view.

```
switch(config-line)#line console 1
switch(config-line)#
```

Related Commands

None

1.3.7 line vty

Function

The **line vty** command displays the virtual terminal (Telnet connection) view.

Format

Global configuration view, line configuration view:

- **line vty** *vty-number*
- **line vty** *vty-number1 vty-number2*

Global configuration view:

no line vty *vty-number*

Parameters

Parameter	Description	Value
vty-number	Specifies the number of a virtual terminal.	The value is an integer ranging from 1 to 32.
vty-number1	Specifies the start virtual terminal number for batch configuration.	The value is an integer ranging from 1 to 32.
vty-number2	Specifies the end virtual terminal number for batch configuration.	The value is an integer ranging from 1 to 32.

Default Value

None

View

Global configuration view, line configuration view

Usage Guidelines

After logging in to the switch through Telnet, you can use this command to enter the Telnet terminal configuration view, and then set other attributes of the terminal.
The switch has five virtual terminals by default. That is, five users can log in to the switch through Telnet concurrently.

Example

Configure virtual terminals line vty 1 to 5.

```
switch(config-line)#line vty 1 5
switch(config-line)#
```

Related Commands

None

1.3.8 login authentication

Function

The **login authentication** command configures the authentication mode for user login.
The **no login authentication** command cancels the authentication mode configuration.

Format

- **login authentication local**
- **login authentication aaa method** *name* **auth-type** { **pap** | **chap** | **ascii** }
- **login authorization aaa method** *name*
- **no login authorization aaa method**

Parameters

Parameter	Description	Value
local	Configures local authentication for user login.	-
aaa	Configures AAA authentication for user login.	-
name	Specifies an AAA authentication method name.	The value is a string of up to 32 bytes.
pap | chap | ascii	Indicates the AAA authentication type.	-

Default Value

None

View

Line configuration view

Usage Guidelines

None

Example

Configure AAA authentication for user login.

```
switch(config-line)#login authorization aaa method auth1
switch(config-line)#
```

Related Commands

None

1.3.9 kill vty

Function

The **kill vty** command terminates the connection with a virtual terminal (Telnet or SSH terminal) and resets the terminal.

Format

kill vty *vty-number*

Parameters

Parameter	Description	Value
vty-number	Specifies the number of a virtual terminal.	The value is an integer ranging from 1 to 32.

Default Value

None

View

Global configuration view

Usage Guidelines

Virtual terminals are those connecting to the switch through Telnet or SSH.
The switch has five virtual terminals by default. That is, five users can log in to the switch through Telnet concurrently.

Example

Terminate the connection with virtual terminal line vty 1.

```
switch(config)#kill vty 1
  Are you sure? (y/n) [y]^I
```

```
[OK]
```

Related Commands

None

1.3.10show lines

Function

The **show lines** command displays the number of users that are allowed to log in to the switch and information about the users that have logged in.

Format

- **show lines**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view

Usage Guidelines

None

Example

Display information about the users that have logged in to the switch.

```
switch#show lines
     Line         Location                  Idle         User
*   1   con 1     Console                    00:00:00    admin
    2   vty 1
    3   vty 2
    4   vty 3
    5   vty 4
    6   vty 5
switch#
```

Related Commands

None

1.3.11 timeout

Function

The **timeout** command sets the timeout time of a virtual terminal with no operation performed.
The **no timeout** command restores the timeout time of a virtual terminal with no operation performed to the default value.

Format

- **timeout** *time1*
- **timeout** *time1 time2*
- **no timeout**

Parameters

Parameter	Description	Value
time1	Specifies the timeout time, in minutes.	The value is an integer ranging from 0 to 35791, in minutes.
time2	Specifies the timeout time, in seconds.	The value is an integer ranging from 0 to 59.

Default Value

By default, the timeout time of a virtual terminal with no operation performed is 600s.

View

Line configuration view

Usage Guidelines

This command functions like the screen saver program of a PC. Once a console terminal does not perform any operation within the timeout time, the system will return to the authentication interface. For a Telnet terminal, its connection with the switch will be terminated in this case.

Example

Set the timeout time of a virtual terminal to 5s. That is, the system will return to the authentication interface if there is no input on the terminal within 5s.

```
switch(config-line)#terminal timeout 5
switch(config-line)#
```

Related Commands

None

1.4 File System Configuration Commands

1.4.1 cd

Function

The **cd** command changes the working directory of the current user, enabling the user to switch between different directories.

Format

- **cd**
- **cd** *directory*

Parameters

Parameter	Description	Value
directory	Specifies a file directory.	The value is a string. The directory name is case insensitive and cannot contain any of the following characters: space, wave line (~), asterisk (*), slash (/), back slash (¥), colon (:), and apostrophe (').

Default Value

None

View

Privileged user view, global configuration view

Usage Guidelines

This command enables you to switch between different directories. If you run this command without specifying directory parameter, you will return to the root directory of the file system.
The directory specified in the command must exist; otherwise, the switch displays the following error message:

```
switch#cd abc
  %"Ram:/flash/abc" is not a directory
```

Example

Change the working directory of the current user on the switch from Ram:/flash to Ram:/flash/user.

```
switch#cd
  %Current Directory is "Ram:/flash".
switch#cd user
  %Current Directory is "Ram:/flash/user".
switch#
```

Related Commands

dir

1.4.2 copy

Function

The **copy** command copies the content of one file to another file.

Format

- **copy** *srcfile destfile*

Parameters

Parameter	Description	Value
srcfile	Specifies the path and name of the source file to be copied.	The value is a string.
destfile	Specifies the path and name of the destination file.	The value is a string.

Default Value

None

View

Privileged user view, global configuration view

Usage Guidelines

The paths and names of the source and destination files are case insensitive and cannot contain any of the following characters: space, wave line (~), asterisk (*), slash (/), back slash (¥), and colon (:).
If you do not specify a file name when setting the *destfile* parameter, the destination file will have the same file name as the source file. However, if the source and destination files are in the same directory, the destination file name must be specified; otherwise, the file copy will fail.

Example

Copy the file clock.sys from the root directory of the flash (assuming that this directory is the current working directory) to flash: /user/, and set the destination file name to clock1.sys.

```
switch#copy clock.sys /user/clock1.sys
  %Copying file Ram:/flash/clock.sys -> Ram:/flash/user/clock1.sys
switch#
```

Related Commands

None

1.4.3 del

Function

The **del** command deletes a specified file from the flash.

Format

- **del** *file-name*

Parameters

Parameter	Description	Value
file-name	Specifies a file name.	The value is a string.

Default Value

None

View

Privileged user view, global configuration view

Usage Guidelines

None

Example

Delete the file 123 from the flash.

```
switch(config)#del 123
switch(config)#
```

Related Commands

None

1.4.4 dir

Function

The **dir** command displays the directory and file information in the storage device.

Format

- **dir**
- **dir all**
- **dir tree** *dir*
- **dir tree** *dir* **subtree**
- **dir tree** *dir* **all**
- **dir tree** *dir* **subtree all**

Parameters

Parameter	Description	Value
dir	Specifies a directory.	The value is a string.
[subtree]	It is an optional parameter, indicating to view the directory or subdirectory information.	-

Default Value

None

View

Privileged user view, global configuration view

Usage Guidelines

This command supports fuzzy match with a wildcard *. If the value is not set, the output of this command displays directory and file information of the current path.
The following table describes the Attr values in the dir command output.

Item	Description
d	Indicates a directory. A value without this item indicates a file.
r	Indicates a readable directory or file.
w	Indicates a writable directory or file.
X	Indicates an executable directory or file.

Example

Display information about all files and directories in the current path.

```
switch#dir
Listing Directory Ram:/flash:
    attr      link    uid       gid         size         date         time     name
---------- ---- -------- -------- ---------- ----------- -------- -----
-rwxrwxrwx 1       0          0                  0 2100-01-01 07:18:14 bootparam.sys
-rwxrwxrSx 1       0          0                  0 2100-01-01 07:18:14 clock.sys
drwxrwxrwx 1       0          0               4096 2100-01-01 07:18:14 user/
drwxrwxrwx 1       0          0               4096 2100-01-01 07:33:14 ssh/
-rwxrwxrwx 1       0          0                  0 2100-01-01 07:18:22 swapfile
-rwxrwxrwx 1       0          0                  0 2100-01-01 07:18:14 cfgresultfile
drwxrwxrwx 1       0          0               4096 2100-01-01 07:18:14 ifcfg/
```

```
-rwxrwxrSx 1       0          0                    0 2100-01-01 07:18:18 startcfg
-rwxrwxrwx 1       0          0                    0 2100-01-01 07:18:22 execfile

          6 files, 3 directories, total space:0 bytes
          available space: 16302080 bytes.
switch#
```

Related Commands

None

1.4.5 dir tree

Function

The **dir tree** command displays the content in a directory or its sub-directories.

Format

- **dir tree** *directory*
- **dir tree** *directory* **subtree**
- **dir tree** *directory* **subtree all**

Parameters

Parameter	Description	Value
directory	Specifies a directory name.	The value is a string. The directory name is case sensitive and cannot contain any of the following characters: space, wave line (~), asterisk (*), slash (/), back slash (¥), colon (:), and apostrophe (').

Default Value

None

View

Privileged user view, global configuration view

Usage Guidelines

None

Example

Display the content in the directory user.

```
switch(config)#dir tree user
Listing Directory Ram:/flash/user:
   attr     link    uid       gid       size        date        time     name
```

```
---------- ---- ------- ------- --------- ---------- -------- -----
drwxrwxrwx 1      0       0            4096 2100-01-01 00:00:56 ./
drwxrwxrwx 1      0       0            4096 2100-01-01 00:00:56 ../
drwxrwxrwx 1      0       0            4096 2100-01-01 00:00:52 admin/
drwxrwxrwx 1      0       0            4096 2100-01-01 00:00:52 root/
drwxrwxrwx 1      0       0            4096 2100-01-01 00:00:56 123/

        0 files, 5 directories, total space:0 bytes

        available space: 16285696 bytes.

switch(config)#
```

Related Commands

None

1.4.6 execute

Function

The **execute** command executes batch commands in a batch file.

Format

- **execute** *file-name*

Parameters

Parameter	Description	Value
file-name	Specifies a file name.	The length is up to 255 characters.

Default Value

None

View

Privileged user view, global configuration view

Usage Guidelines

None

Example

Execute batch commands in batch file fs.

```
switch(config)#execute fs
switch(config)#
```

Related Commands

None

1.4.7 mkdir

Function

The **mkdir** command creates a new directory.

Format

mkdir *directory*

Parameters

Parameter	Description	Value
directory	Specifies the name of the new directory.	The value is a string. The directory name is case sensitive and cannot contain any of the following characters: space, wave line (~), asterisk (*), slash (/), back slash (¥), colon (:), and apostrophe (').

Default Value

None

View

Privileged user view, global configuration view

Usage Guidelines

None

Example

Create a new directory fs under %"Ram:/flash/.

```
switch#mkdir fs
switch#
```

Related Commands

None

1.4.8 move

Function

The **move** command moves a source file or wildcard to the target file or directory.

Format

- **move** *srcfile destfile*

Parameters

Parameter	Description	Value
srcfile	Specifies the source file.	The length is up to 255 characters.
destfile	Specifies the target file.	The length is up to 255 characters.

Default Value

None

View

Privileged user view, global configuration view

Usage Guidelines

None

Example

Move source file fs to the dmp directory.

```
switch#move fs dmp
switch#
```

Related Commands

None

1.4.9 pwd

Function

The **pwd** command displays the current directory.

Format

pwd

Parameters

None

Default Value

None

View

Privileged user view, global configuration view

Usage Guidelines

None

Example

Display the current directory.

```
switch#pwd
  %Current Directory is "Ram:/flash".
switch#
```

Related Commands

None

1.4.10remove

Function

The **remove** command deletes a specified file from the storage device of the switch in a recoverable manner.

Format

- **remove** *file-name*

Parameters

Parameter	Description	Value
file-name	Specifies the path and name of the file to be deleted.	The value is a string. The directory name is case insensitive and cannot contain any of the following characters: space, wave line (~), asterisk (*), slash (/), back slash (¥), colon (:), and apostrophe (').

Default Value

None

View

Privileged user view, global configuration view

Usage Guidelines

This command supports fuzzy match with a wildcard .

Example

Delete files in the directory TEMP on the core switch card.

```
switch#remove TEMP
switch#
```

Related Commands

None

1.4.11 rename

Function

The **rename** command renames a file.

Format

- **rename** *src-filename new-filename*

Parameters

Parameter	Description	Value
src-filename	Specifies original file name.	The value is a string. The file name is case insensitive and cannot contain any of the following characters: space, wave line (~), asterisk (*), slash (/), back slash (¥), colon (:), and apostrophe (').
new-filename	Specifies the new file name.	The value is a string. The file name is case insensitive and cannot contain any of the following characters: space, wave line (~), asterisk (*), slash (/), back slash (¥), colon (:), and apostrophe (').

Default Value

None

View

Privileged user view, global configuration view

Usage Guidelines

If the new file name is the same as an existing directory name or file name, the system will display an error message.
If the values of *src-filename* and *new-filename* do not contain the directory of the file to be renamed, ensure that the file is saved in the working directory of the current user.

Example

Change the name of the file sample.txt to sample.bak.

```
switch#rename sample.txt sample.bak
```

```
switch#
```

Related Commands

None

1.4.12rmdir

Function

The **rmdir** command deletes a directory or its sub-directories.

Format

- **rmdir** *directory*
- **rmdir** *directory* **subtree**

Parameters

Parameter	Description	Value
directory	Specifies the name of the directory to be deleted.	The value is a string. The directory name is case sensitive and cannot contain any of the following characters: space, wave line (~), asterisk (*), slash (/), back slash (¥), colon (:), and apostrophe (').

Default Value

None

View

Privileged user view, global configuration view

Usage Guidelines

None

Example

Delete the directory 123.

```
switch#rmdir 123
switch#ls
Listing Directory Ram:/flash:
    attr      link     uid        gid         size         date          time     name
---------- ---- ------- ------- --------- ---------- -------- -----
-rwxrwxrwx 1       0          0                    0 2100-01-01 00:43:08 bootparam.sys
-rwxrwxrSx 1       0          0                    0 2100-01-01 00:43:08 clock.sys
drwxrwxrwx 1       0          0                 4096 2100-01-01 00:43:08 user/
-rwxrwxrwx 1       0          0                    0 2100-01-01 00:43:26 execfile
```

```
-rwxrwxrwx 1       0          0                  0 2100-01-01 00:43:26 swapfile
-rwxrwxrwx 1       0          0                  0 2100-01-01 00:43:08 cfgresultfile
drwxrwxrwx 1       0          0               4096 2100-01-01 00:43:08 ifcfg/
-rwxrwxrSx 1       0          0                  0 2100-01-01 00:43:10 startcfg

          6 files, 2 directories, total space:0 bytes
          available space: 16318464 bytes.
switch#
```

Related Commands

None

1.4.13type

Function

The **type** command displays the content of a specified binary or text file. The file system displays the file content in a text file.

Format

- **type** *file*-name
- **type** *file*-name { **binary** | **text** }

Parameters

Parameter	Description	Value
file-name	Specifies the specific file name.	The value is a string.
binary	Specifies a binary file name.	The value is a string. The file name is case insensitive and cannot contain any of the following characters: space, wave line (~), asterisk (*), slash (/), back slash (¥), colon (:), and apostrophe (').
text	Specifies a text file name.	The value is a string. The file name is case insensitive and cannot contain any of the following characters: space, wave line (~), asterisk (*), slash (/), back slash (¥), colon (:), and apostrophe (').

Default Value

None

View

Privileged user view, global configuration view

Usage Guidelines

The file system of the switch displays files in the text format. If you do not specify the file directory in the command, the system defaults the directory as the current directory.
You can use the dir or ls command in the current view to obtain the name of the file you want to check.

Example

Display the content of the text file startcfg.

```
switch#type startcfg
!System startup configuration
!version V310R230
!2019/01/09 00:18:18
!
 hostname switch
 no auth-degenerate
!
 logging history 7
!
 username admin group administrators password 827ccb0eea8a706c4c34a16891f84e7b
 user reauth-interval 10
 user fail-count 10
 user privilege level administrators password 306b6341993337d4
 user privilege level operators password 306b6341993337d4
 user privilege level users password 306b6341993337d4
 user privilege level guests password 306b6341993337d4
!
 snmp trap-history 1024
 snmp rich-trap enable
!
 vlan 1
!
interface mgt-eth 0/0/0
!
 voice-vlan oui 00:01:e3:00:00:00/24 "Simens phone"
 voice-vlan oui 00:03:6b:00:00:00/24 "Cisco phone"
 voice-vlan oui 00:04:0d:00:00:00/24 "Avaya phone"
 voice-vlan oui 00:60:b9:00:00:00/24 "Philips/NEC phone"
 voice-vlan oui 00:d0:1e:00:00:00/24 "Pingtel phone"
 voice-vlan oui 00:e0:75:00:00:00/24 "Polycom phone"
 voice-vlan oui 00:e0:bb:00:00:00/24 "3Com phone"
!
line console 1
```

```
 length 24
 timeout 0 0
 login local
 language english
 no color
line vty 1 5
 length 24
 no monitor
 timeout 10 0
 login local
 language english
 no color
!
!
interface 100gigaethernet 1/0/1
!
interface 100gigaethernet 1/0/2
!
interface 100gigaethernet 1/0/3
!
interface 100gigaethernet 1/0/4
!
interface 100gigaethernet 1/0/5
!
interface 100gigaethernet 1/0/6
!
interface 100gigaethernet 1/0/7
!
interface 100gigaethernet 1/0/8
!
interface 100gigaethernet 1/0/9
!
interface 100gigaethernet 1/0/10
!
interface 100gigaethernet 1/0/11
!
interface 100gigaethernet 1/0/12
!
interface 100gigaethernet 1/0/13
!
interface 100gigaethernet 1/0/14
```

```
!
interface 100gigaethernet 1/0/15
!
interface 100gigaethernet 1/0/16
!
interface 100gigaethernet 1/0/17
!
interface 100gigaethernet 1/0/18
!
interface 100gigaethernet 1/0/19
!
interface 100gigaethernet 1/0/20
!
interface 100gigaethernet 1/0/21
!
interface 100gigaethernet 1/0/22
!
interface 100gigaethernet 1/0/23
!
interface 100gigaethernet 1/0/24
!
interface 100gigaethernet 1/0/25
!
interface 100gigaethernet 1/0/26
!
interface 100gigaethernet 1/0/27
!
interface 100gigaethernet 1/0/28
!
interface 100gigaethernet 1/0/29
!
interface 100gigaethernet 1/0/30
!
interface 100gigaethernet 1/0/31
!
interface 100gigaethernet 1/0/32
!
interface 10gigaethernet 1/0/33
!
interface 10gigaethernet 1/0/34
!end
```

```
switch#
```

Related Commands

dir

1.4.14xcopy

Function

The x**copy** command copies one folder to another folder.

Format

- **xcopy** *srcfile destfile*

Parameters

Parameter	Description	Value
srcfile	Specifies the path and name of the source folder to be copied.	The value is a string.
destfile	Specifies the path and name of the destination folder.	The value is a string.

Default Value

None

View

Privileged user view, global configuration view

Usage Guidelines

The paths and names of the source and destination folders are case insensitive and cannot contain any of the following characters: space, wave line (~), asterisk (*), slash (/), back slash (¥), and colon (:).

Example

Copy the folder clock from the root directory of the flash (assuming that this directory is the current working directory) to flash: /user/.

```
switch#xcopy clock /user/clock1.sys
  %Copying file Ram:/flash/clock -> Ram:/flash/user/clock
switch#
```

Related Commands

None

1.4.15zero

Function

The **zero** command deletes all content of a specified file.

Format

zero *filename*

Parameters

Parameter	Description	Value
filename	Specifies the path and name of the file of which the content will be deleted.	The value is a string. The file name is case insensitive and cannot contain any of the following characters: space, wave line (~), asterisk (*), slash (/), back slash (¥), colon (:), and apostrophe (').

Default Value

None

View

Privileged user view, global configuration view

Usage Guidelines

None

Example

Deletes all the content of the file temp.

```
switch#zero temp
switch#
```

Related Commands

dir

1.5 System Configuration File Commands

1.5.1 auth-degenerate

Function

The **auth-degenerate enable** command changes the authentication mode to local authentication.
The **no auth-degenerate disable** command cancels the configuration.

Format

- **auth-degenerate**
- **no auth-degenerate**

Parameters

None

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Change the authentication mode to local configuration.

```
switch(config)#auth-degenerate
switch(config)#
```

1.5.2 erase startup-config

Function

The **erase startup-config** command deletes the startup configuration file in the storage device of the switch.

Format

erase startup-config

Parameters

None

Default Value

None

View

Privileged user view, global configuration view

Usage Guidelines

This command is usually used in either of the following conditions:
After the system software of the switch is upgraded, the configuration file saved in the storage does not match the new software version. In this case, run this command to delete the old startup configuration file.
When the switch is used in a new environment, the original configuration file does not meet requirements of the new application. In this case, you need to delete the old startup configuration file and re-configure the switch.

If you do not use the write file command to save the configuration after running this command, the system will be initialized with the default configuration after the next startup.

Warning: It is recommended that this command be used under instruction of technical support personnel.

Example

Delete the startup configuration file in the storage device.

```
switch(config)#erase startup-config
  This will erase the configuration in the flash memory.
  Are you sure? (y/n) [y] y
switch(config)#
```

Related Commands

show running-config, write file

1.5.3 show running-config

Function

The **show running-config** command displays the running system configuration.

Format

- **show running-config**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view

Usage Guidelines

After completing a series of configuration, you can run this command to check whether the running system configuration is correct.

Example

Display the running system configuration.

```
switch#show running-config
!Device running configuration:
!version V310R230
!2019/08/18 13:32:54
```

```
!
 no auth-degenerate
!
 username admin group administrators password $1$kijv$blP5gEaeX6wG6eQLeT3Di0
 username super group administrators password $1$kijv$blP5gEaeX6wG6eQLeT3Di0
 user privilege level administrators password $9$kijv$e7015e4ca31c3ae839aa564bc4b0f361
 user privilege level operators password $9$kijv$e7015e4ca31c3ae839aa564bc4b0f361
 user privilege level users password $9$kijv$e7015e4ca31c3ae839aa564bc4b0f361
 user privilege level guests password $9$kijv$e7015e4ca31c3ae839aa564bc4b0f361
!
 hostname switch
!
 management acl enable
!
 temperature 1 trap disable
 temperature 2 trap disable
 temperature 3 trap disable
!
 voltage trap 1 disable
 voltage trap 2 disable
!
 power 1 trap disable
 power 2 trap disable
!
 filter-list 1
 filter-list 1001
 filter-list 2001
 filter-list 3001
 --More--
switch#
```

Related Commands

show running-config, erase startup-config, write file

1.5.4 show startup-config

Function

The **show startup-config** command displays the configuration file used upon the next startup of the switch.

Format

- **show startup-config**
- **show startup-config** { **include** | **exclude**| **begin** } **substring** *string*

Parameters

Parameter	Description	Value
string	Specifies a string used for filtering the configuration information to be displayed.	The value is a string.

Default Value

None

View

Common user view, privileged user view, global configuration view

Usage Guidelines

The startup configuration file is the configuration file that the switch uses when it is powered on or reboots.
If the switch is powered on successfully but does not work normally after entering CLI, you can use this command to check the startup configuration file.
If no configuration file is saved in the system, this command cannot display any information.

Example

Display the configuration file used upon the next startup of the switch.

```
switch#show startup-config
!System startup configuration
!version V310R230
!2019/08/16 09:09:02
!
 no auth-degenerate
!
 username admin group administrators password $1$kijv$blP5gEaeX6wG6eQLeT3Di0
 username super group administrators password $1$kijv$blP5gEaeX6wG6eQLeT3Di0
 user privilege level administrators password $9$kijv$e7015e4ca31c3ae839aa564bc4b0f361
 user privilege level operators password $9$kijv$e7015e4ca31c3ae839aa564bc4b0f361
 user privilege level users password $9$kijv$e7015e4ca31c3ae839aa564bc4b0f361
 user privilege level guests password $9$kijv$e7015e4ca31c3ae839aa564bc4b0f361
!
 hostname switch
!
 temperature 1 trap disable
 temperature 2 trap disable
 temperature 3 trap disable
!
 voltage trap 1 disable
```

```
 voltage trap 2 disable
!
vlan 1
!
interface mgt-eth 0/0/0
!
interface vlan 1
 ip address 10.82.20.211/16
!
 gratuitous-arp learning enable
!
 syslog facility kernel
!
 snmp community $9$kijv$c1a221701187cd8ec25a10484d937b5b rw view internet
 no snmp community private
!
line console 1
 length 24
 timeout 10 0
 login authentication local
 language english
 no color
line vty 1 5
 length 24
 no monitor
 timeout 10 0
 login authentication local
 language english
 no color
!
!
interface 100gigaethernet 1/0/1
!
interface 100gigaethernet 1/0/2
!
interface 100gigaethernet 1/0/3
!
interface 100gigaethernet 1/0/4
!
interface 100gigaethernet 1/0/5
!
```

```
interface 100gigaethernet 1/0/6
!
interface 100gigaethernet 1/0/7
!
interface 100gigaethernet 1/0/8
!
interface 100gigaethernet 1/0/9
!
interface 100gigaethernet 1/0/10
!
interface 100gigaethernet 1/0/11
!
interface 100gigaethernet 1/0/12
!
interface 100gigaethernet 1/0/13
!
interface 100gigaethernet 1/0/14
!
interface 100gigaethernet 1/0/15
!
interface 100gigaethernet 1/0/16
!
interface 100gigaethernet 1/0/17
!
interface 100gigaethernet 1/0/18
!
interface 100gigaethernet 1/0/19
!
interface 100gigaethernet 1/0/20
!
interface 100gigaethernet 1/0/21
!
interface 100gigaethernet 1/0/22
!
interface 100gigaethernet 1/0/23
!
interface 100gigaethernet 1/0/24
!
interface 100gigaethernet 1/0/25
!
interface 100gigaethernet 1/0/26
```

```
!
interface 100gigaethernet 1/0/27
!
interface 100gigaethernet 1/0/28
!
interface 100gigaethernet 1/0/29
!
interface 100gigaethernet 1/0/30
!
interface 100gigaethernet 1/0/31
!
interface 100gigaethernet 1/0/32
!
interface 10gigaethernet 1/0/33
!
interface 10gigaethernet 1/0/34
!
ip route-static 0.0.0.0 0.0.0.0 10.82.1.254
!
!
!end

switch#
```

Related Commands

show startup-config

1.5.5 write file

Function

The **write file** command saves the current system configuration in the startup configuration file.

Format

- **write file**

Parameters

None

Default Value

None

View

Privileged user view

Usage Guidelines

You do not need to specify the path of the startup configuration file because the path has been written in the system.
If you want to permanently use a series of configuration you complete, run this command to save the configuration in the current startup configuration file.

Example

Save the current system configuration in the startup configuration file.

```
switch#write file
  This will save the configuration in the flash memory.
  Are you sure? (y/n) [y]y
  Building configuration, please wait for a moment...
  Begin to write.
  Finishing writing the configuration file.

  [OK]
switch#
```

Related Commands

erase startup-config, show running-config

1.6 File Uploading and Downloading Configuration Commands

1.6.1 tftp get

Function

The **tftp get** command downloads a remote file using the TFTP protocol and saves it on the local device. (This command applies to IPv4 networks.)

Format

- **tftp get** *ipv4-address remotefile* [*port-id*]
- **tftp get** *ipv4-address remotefile* **localfile** *filename* [*port-id*]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of the TFTP server.	The value is in dotted decimal notation.
remotefile	Specifies a file name on the TFTP server.	The value is a string of 1 to 63 characters.

Parameter	Description	Value
filename	Specifies a local file name.	The value is a string of 1 to 63 characters.
port-id	Specifies the port number of the TFTP server. This parameter is optional.	The value is an integer ranging from 1 to 65535.

Default Value

None

View

Global configuration view

Usage Guidelines

During device operation and maintenance, you may need to download configuration files or operating system files to the switch from a host (TFTP server) to modify the configuration or upgrade the operating system. This command is used to download such files to the switch.
If you do not specify *filename* in the command, the downloaded file will have the same name as the file on the TFTP server.
Before running this command, ensure that the switch can communicate with the TFTP server, and the user name and password have been configured on the TFTP server.

Note: It is recommended that you use this command under instruction of technical support personnel.

Example

Download the file switch_OS.bin to the switch from the TFTP server, and save the file on the switch as v2.4.bin.

```
switch(config)#tftp get 192.168.1.2 onie-installer
 Local path is "/ram/download".
 Getting data...
 198063382 bytes downloaded    %Transmission success.
```

Related Commands

tftp put

1.6.2 tftp put

Function

The **tftp put** command uploads a local file to a remote TFTP server. (This command applies to IPv4 networks.)

Format

- **tftp put** *ipv4-address remotefile* **config**
- **tftp put** *ipv4-address remotefile* **running-config**
- **tftp put** *ipv4-address remotefile* **localfile** *filename* [*port-id*]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of the TFTP server.	The value is in dotted decimal notation.
remotefile	Specifies the file name used after the local file is uploaded to the TFTP server.	The value is a string of 1 to 63 characters.
filename	Specifies the name of the local file to be uploaded.	The value is a string of 1 to 63 characters.
port-id	Specifies the port number of the TFTP server. This parameter is optional.	The value is an integer ranging from 1 to 65535.
config	Uploads the configuration file of the switch.	-

Default Value

None

View

Global configuration view

Usage Guidelines

During device operation and maintenance, you can use this command to upload files of the switch (including the configuration file) to a remote TFTP server for backup.
Before running this command, ensure that the switch can communicate with the TFTP server, and the user name and password have been configured on the TFTP server. In addition, the user account must have the read and write permissions on the TFTP server. Otherwise, the host will not respond for a long time or the upload task will be suspended.

Note: It is recommended that you use this command under instruction of technical support personnel.

Example

Upload the configuration file of the switch to the TFTP server, and save the file as config.ini on the server.

```
switch(config)#tftp put 10.18.33.127 d:/config.ini config
 1136 bytes uploaded
switch(config)#
```

1.6.3 tftpd

Function

The **tftpd** command enables the TFTP server function on the switch.
The **no tftpd** command disables the TFTP server function on the switch.

Format

- **tftpd**

- **no tftpd**

Parameters

None

Default Value

By default, the TFTP server function is disabled.

View

Global configuration view

Usage Guidelines

After the TFTP server function is enabled on the switch, the switch acts as a TFTP server. You can log in to the switch using a TFTP client and upload files to or download files from the switch. The TFTP server uses the local user name and password for login authentication.

Example

Enable the TFTP server function on the switch.

```
switch(config)#tftpd
  %TFTP server successfully start!
switch(config)#
```

1.6.4 ftp delete

Function

The **ftp delete** command deletes a file from a specified FTP server. (This command applies to IPv4 networks.)

Format

- **ftp delete** *ipv4-address user password remotefile*
- **ftp delete** *ipv4-address user password remotefile port-id*

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of the FTP server.	The value is in dotted decimal notation.
user	Specifies the user name used to log in to the FTP server.	The value is a string of 1 to 63 characters.
password	Specifies the password used to log in to the FTP server.	The value is a string of 1 to 63 characters.
remotefile	Specifies a file name on the FTP server.	The value is a string of 1 to 63 characters.

Parameter	Description	Value
port-id	Specifies the port number of the FTP server. This parameter is optional.	The value is an integer ranging from 1 to 65535.

Default Value

None

View

Global configuration view

Usage Guidelines

Note: It is recommended that you use this command under instruction of technical support personnel.

Example

Delete the files on the specified FTP server

```
switch(config)#ftp delete 10.18.2.16 aaa 111 rem 11
switch(config)#
```

1.6.5 ftp get

Function

The **ftp get** command downloads a remote file and saves it on the local device. (This command applies to IPv4 networks.)

Format

Common user view, global configuration view:

- **ftp get** *ipv4-address user password remotefile* [*port-id*]
- **ftp get** *ipv4-address user password remotefile* **localfile** *filename* [*port-id*]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of the FTP server.	The value is in dotted decimal notation.
user	Specifies the user name used to log in to the FTP server.	The value is a string of 1 to 63 characters.
password	Specifies the password used to log in to the FTP server.	The value is a string of 1 to 63 characters.
remotefile	Specifies a file name on the FTP server.	The value is a string of 1 to 63 characters.
filename	Specifies a local file name.	The value is a string of 1 to 63 characters.
port-id	Specifies the port number of the FTP server.	The value is an integer ranging from 1

Parameter	Description	Value
	This parameter is optional.	to 65535.

Default Value

None

View

Common user view, global configuration view

Usage Guidelines

During device operation and maintenance, you may need to download configuration files or operating system files to the switch from a host (FTP server) to modify the configuration or upgrade the operating system. This command is used download such files to the switch.
If you do not specify *filename* in the command, the downloaded file will have the same name as the file on the FTP server.
Before running this command, ensure that the switch can communicate with the FTP server, and the user name and password have been configured on the FTP server.

Note: It is recommended that you use this command under instruction of technical support personnel.

Example

Use the user name 123 and password 123 to log in to the FTP server with IP address 192.168.1.200, download the file switch.bin to the switch from the FTP server, and save the file on the switch as v2.4.bin.

```
switch(config)#ftp get 192.168.1.200 123 123 switch.bin localfile v2.4.bin
 Getting File “switch.bin” from 192.168.1.200...
 1528618 bytes downloaded.
 If you want to upgrade system, use “upgrade” command!
switch(config)#
```

Related Commands

ftp put

1.6.6 ftp put

Function

The **ftp put** command uploads a local file to a remote FTP server. (This command applies to IPv4 networks.)

Format

- **ftp put** *ipv4-address user password remotefile* **config**
- **ftp put** *ipv4-address user password remotefile* **running-config**
- **ftp put** *ipv4-address user password remotefile* **localfile** *filename* [*port-id*]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of the FTP server.	The value is in dotted decimal notation.
user	Specifies the user name used to log in to the FTP server.	The value is a string of 1 to 63 characters.
password	Specifies the password used to log in to the FTP server.	The value is a string of 1 to 63 characters.
remotefile	Specifies a file name on the FTP server.	The value is a string of 1 to 63 characters.
filename	Specifies a local file name.	The value is a string of 1 to 63 characters.
port-id	Specifies the port number of the FTP server. This parameter is optional.	The value is an integer ranging from 1 to 65535.
config	Uploads the configuration file of the switch.	-

Default Value

None

View

Global configuration view

Usage Guidelines

During device operation and maintenance, you can use this command to upload files of the switch (including the configuration file) to a remote FTP server for backup.
Before running this command, ensure that the switch can communicate with the FTP server, and the user name and password have been configured on the FTP server. In addition, the user account must have the read and write permissions on the FTP server. Otherwise, the host will not respond for a long time or the upload task will be suspended.

Note: It is recommended that you use this command under instruction of technical support personnel.

Example

Use the user name 123 and password 123 to log in to the FTP server with IP address 192.168.1.200, upload the configuration file of the switch to the FTP server, and save the file as config.ini on the server.

```
switch(config)#ftp put 192.168.1.200 123 123 d:/config.ini config
 1136 bytes uploaded
switch(config)#
```

1.7 Telnet and SSH Configuration Commands

1.7.1 debug ssh

Function

The **debug ssh** command enables SSH debugging.

The **no debug ssh** command disables SSH debugging.

Format

- **debug ssh**
- **no debug ssh**

Parameters

None

Default Value

By default, SSH debugging is disabled.

View

Privileged user view

Usage Guidelines

None

Example

Enable SSH debugging.

```
switch#debug ssh
switch#
```

1.7.2 sshd

Function

The **sshd** command enables the SSH function on the switch.
The **no sshd** command cancels the configuration.

Format

- **sshd**
- **no sshd**

Parameters

None

Default Value

By default, the SSH function is disabled.

View

Global configuration view

Usage Guidelines

After the switch is powered on for the first time, you must log in to the switch through the console interface, enable the SSH function, and complete related SSH configuration, so that users can log in to the switch using SSH later. Generally, SSH login is used when there are relatively high security requirements for user login.

Example

Enable the SSH function on the switch.

```
switch(config)#sshd
switch(config)#
```

1.7.3 sshd auth

Function

The **sshd auth** command sets the SSH authentication mode, including password authentication and public key authentication.

Format

- **sshd auth** { **password** | **pubkey** }
- **no sshd auth** { **password** | **pubkey** }

Parameters

None

Default Value

By default, the system supports both password authentication and public key authentication.

View

Global configuration view

Usage Guidelines

This command sets the SSH authentication mode. Password authentication and public key authentication can coexist. Configuring public key authentication will not disable password authentication, and configuring password authentication will not disable public key authentication.

Example

Set the SSHD authentication mode to password authentication.

```
switch(config)#sshd auth password
switch(config)#
```

1.7.4 sshd login-grace-time

Function

The **sshd login-grace-time** command configures the SSHd login grace time.

Format

- **sshd login-grace-time** { *login-grace-timer* | **default** }

Parameters

Parameter	Description	Value
login-grace-timer	Specifies the validity period of SSH login.	The value is an integer ranging from 60 to 600, in seconds.
default	Restores the default validity period of SSH login.	The value is 300s.

Default Value

The default value is 300s.

View

Global configuration view

Usage Guidelines

After you connect to the switch through SSH, the system displays the validity period to enter the user name and password. If you do not enter the user name and password within this period, the login authentication fails.

Example

Set the SSHd login grace time to 400s.

```
switch(config)#sshd login-grace-time 400
switch(config)#
```

1.7.5 telnetd (IPv4)

Function

The **telnetd** command enables the IPv4 Telnet service.
The **no telnetd** command disables the IPv4 Telnet service.

Format

- **telnetd**
- **no telnetd**

Parameters

None

Default Value

By default, the IPv4 Telnet service is enabled.

View

Global configuration view

Usage Guidelines

After the IPv4 Telnet service is enabled, you can remotely configure and manage the device. To ensure device safety, you can set the Telnet service access list for IPv4 addresses, to ensure that trusted persons can configure and maintain the device and protect the device from remote attacks to the Telnet service with IPv4 addresses.

Example

Disable the IPv4 Telnet service.

```
switch(config)#no telnetd
switch(config)#
```

1.7.6 telnet6d

Function

The **telnet6d** command enables the IPv6 Telnet service.
The **no telnet6d** command disables the IPv6 Telnet service.

Format

- **telnet6d**
- **no telnet6d**

Parameters

None

Default Value

By default, the IPv6 Telnet service is enabled.

View

Global configuration view

Usage Guidelines

After the IPv6 Telnet service is enabled, you can remotely configure and manage the device. To ensure device safety, you can set the Telnet service access list for IPv6 addresses, to ensure that trusted persons can configure and maintain the device and protect the device from remote attacks to the Telnet service with IPv6 addresses.

Example

Disable the IPv6 Telnet service.

```
switch(config)#no telnet6d
switch(config)#
```

1.7.7 telnet|telnet6

Function

The **telnet|telnet6** command enables you to log in to a remote device.

Format

- **telnet** *ipv4-address* [*port-id*]
- **telnet** *ipv4-address* **-s** *src-ipv4-address* [*port-id*]
- **telnet** *ipv4-address* **vpn-instance** *name* [*port-id*]
- **telnet** *ipv4-address* **vpn-instance** *name* **-s** *src-ipv4-address* [*port-id*]
- **telnet** *mac-address* [*port-id*]
- **telnet6** *ipv6-address* [*port-id*]
- **telnet6** *ipv6-address* **-s** *src-ipv6-address* [*port-id*]
- **telnet6** *ipv6-address* **vpn-instance** *name* [*port-id*]
- **telnet6** *ipv6-address* **vpn-instance** *name* **-s** *src-ipv6-address* [*port-id*]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IP address of the device you want to log in.	The value is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of the device you want to log in.	A 128-bit IPv6 address is divided into 8 groups, with 16 bits in each group. Each group is expressed by four hexadecimal digits (0-9 and A-F), and two groups are separated with a colon (:). Each X represents a group of hexadecimal digits.
src-ipv4-address	Specifies a source IPv4 address.	The value is in dotted decimal notation.
src-ipv6-address	Specifies a source IPv6 address.	A 128-bit IPv6 address is divided into 8 groups, with 16 bits in each group. Each group is expressed by four hexadecimal digits (0-9 and A-F), and two groups are separated with a colon (:). Each X represents a group of hexadecimal digits.
port-id	Specifies the Telnet port number. This parameter is optional.	The value is an integer ranging from 1 to 65535.
name	Specifies a VPN instance name.	The value is a string.

Default Value

None

View

Privileged user view

Usage Guidelines

None

Example

Remotely log in to the switch with IP address 10.18.14.249.

```
switch#telnet 10.18.16.249
Login authentication
Username:
```

Related Commands

None

1.7.8 show ssh config

Function

The **show ssh config** command displays the SSH configuration on the switch.

Format

show ssh config

Parameters

None

Default Value

None

View

Privileged user view, global configuration view

Usage Guidelines

None

Example

Display the SSH configuration.

```
switch(config)#show ssh config
sshd
switch(config)#
```

2. Ethernet Commands

2.1 Overview

This chapter introduces the Ethernet configuration commands of the N-series switch.

2.2 Interface Configuration Commands

2.2.1 alias

Function

The **alias** command sets the alias (description) of an interface.
The **no alias** command cancels the alias configuration of an interface.

Format

- **alias** *alias-name*
- **no alias**

Parameters

Parameters	Description	Value
alias-name	Specifies an alias of the interface.	The value is a string of 1 to 128 characters without spaces.

Default Value

None

View

Interface configuration view (10GE/25GE/100GE/Trunk interface), VLAN configuration view, VLANIF configuration view, and interface group configuration view.

Usage Guidelines

None

Example

Set an alias for an interface.

```
switch(config)#interface 10gigaethernet 1/0/1
switch(config-10ge1/0/1)#alias Delaware
switch(config-10ge1/0/1)#quit
```

2.2.2 duplex

Function

The **duplex** command sets the duplex mode of a fast Ethernet interface.

Format

- **duplex** { **full** | **default** }

Parameters

Parameters	Description	Value
full	Specifies the full duplex mode.	-
default	Uses the default duplex mode, namely, full duplex.	-

Default Value

By default, a fast Ethernet interface works in the default duplex mode (full duplex).

View

Interface configuration view (10/25/100Gigabit Ethernet) and interface group configuration view

Usage Guidelines

On a network, interconnected interfaces should work in the same mode.

Example

Configure interface 10gigaethernet 1/0/1 to work in full duplex mode.

```
switch(config-10ge1/0/1)#duplex full
switch(config-10ge1/0/1)
```

2.2.3 error-down auto-recovery cause bpdu-protection interval

Function

The **error-down auto-recovery cause bpdu-protection interval** command enables the STP BPDU protection, so as to automatically restore an interface in "down" state to "up" state. This command also sets the hold-off time for the automatic restoration.
The **no error-down auto-recovery cause bpdu-protection** command disables the function.

Format

- **error-down auto-recovery cause bpdu-protection interval** *interval*
- **no error-down auto-recovery cause bpdu-protection**

Parameters

Parameters	Description	Value
interval	Specifies the hold-off time for automatically restoring the interface state to "up".	The value is an integer in the range from 30 to 86400, in seconds. Smaller the value, shorter the hold-off

Parameters	Description	Value
		time, and higher the flapping frequency of the interface status (up / down). Larger the value, longer the hold-off time, and longer the duration of interface traffic interruption.

Default Value

enable

View

Global configuration view

Usage Guidelines

In the network running STP, if an edge interface is configured with the BPDU protection and someone forged BPDU messages to maliciously attack the switch, the switch will turn the edge interface status to "down" when receiving BPDU messages. In this way, all the services on this interface is blocked. This command sets the hold-off time for automatically restoring the interface state to "up" after the interface is disabled by the BPDU protection.

Example

Enable the STP BPDU protection, so as to automatically restore an interface in "down" state to "up" state, and set the hold-off time of automatically restoration to 50s.

```
switch(config)#error-down auto-recovery cause bpdu-protection interval 50
switch(config)#
```

2.2.4 error-down auto-recovery cause mac-address-flapping

Function

The **error-down auto-recovery cause mac-address-flapping interval** command restores an interface to up state when it is becomes down due to MAC address flapping. This command also sets the hold-off time for the automatic restoration.
The **no error-down auto-recovery cause mac-address-flapping** command disables the function.

Format

- **error-down auto-recovery cause mac-address-flapping interval** *interval*
- **no error-down auto-recovery cause mac-address-flapping**

Parameters

Parameters	Description	Value
interval	Specifies the hold-off time for automatically restoring the interface state to "up".	The value is an integer in the range from 30 to 86400, in seconds. Smaller the value, shorter the hold-off

Parameters	Description	Value
		time, and higher the flapping frequency of the interface status (up / down). Larger the value, longer the hold-off time, and longer the duration of interface traffic interruption.

Default Value

Enable

View

Global configuration view

Usage Guidelines

None

Example

Restore an interface to up state when it is becomes down due to MAC address flapping, and set the hold-off time of automatically restoration to 50s.

```
switch(config)#error-down auto-recovery cause mac-address-flapping interval 50
switch(config)#
```

2.2.5 error-down auto-recovery cause storm-suppression interval

Function

The **error-down auto-recovery cause storm-suppression interval** command configures the interval for automatically restoring an interface disabled by storm suppression to "up" state.
The **no error-down auto-recovery cause storm-suppression** command disables the function.

Format

- **error-down auto-recovery cause storm-suppression interval** *interval*
- **no error-down auto-recovery cause storm-suppression**

Parameters

Parameters	Description	Value
interval	Specifies the hold-off time for automatically restoring the interface state to "up".	The value is an integer in the range from 30 to 86400, in seconds. Smaller the value, shorter the hold-off time, and higher the flapping frequency of the interface status (up / down). Larger the value, longer the hold-off time,

Parameters	Description	Value
		and longer the duration of interface traffic interruption.

Default Value

Enable

View

Global configuration view

Usage Guidelines

If the suppression action of an interface on the switch is set to "error-down", and the average receiving rate of broadcast, multicast or unknown unicast packets on the interface exceeds the threshold within the storm suppression detection interval, the interface will be disabled.

Example

Set the interval to 50s for automatically restoring an interface disabled by storm suppression to "up" state.

```
switch(config)#error-down auto-recovery cause storm-suppression interval 50
switch(config)#
```

2.2.6 error-down auto-recovery cause transceiver-power-low interval

Function

The **error-down auto-recovery cause transceiver-power-low interval** command configures the interval for automatically restoring an interface to "up" state from "down" status caused by over-low interface optical power.
The **no error-down auto-recovery cause transceiver-power-low** command disables the function.

Format

- **error-down auto-recovery cause transceiver-power-low interval** *interval*
- **no error-down auto-recovery cause transceiver-power-low**

Parameters

Parameters	Description	Value
interval	Specifies the hold-off time for automatically restoring the interface state to "up".	The value is an integer in the range from 30 to 86400, in seconds. Smaller the value, shorter the hold-off time, and higher the flapping frequency of the interface status (up / down). Larger the value, longer the hold-off time, and longer the duration of interface traffic interruption.

Default Value

Enable

View

Global configuration view

Usage Guidelines

None

Example

Configure the interval for the interface turning into "up" state from "down" state to 50s. The state change is caused by over-low interface optical power.

```
switch(config)#error-down auto-recovery cause transceiver-power-low interval 50
switch(config)#
```

2.2.7 fec

Function

The **fec** command can be used to configure the interface FEC mode.

Format

- **fec mode (rs|base-r|none)**

Parameters

Parameters	Description	Value
rs	Enable the RS FEC function on an interface	-
base-r	Enable the Base-R FEC function on an interface	-
none	FEC is disabled	-

Default Value

By default, the interface works at None.

View

Interface configuration view .

Usage Guidelines

If FEC is enabled at one end of a link, this function must also be enabled at the other end of the link.

Note: Configure on 25G and 100G interfaces.

Example

#Configuration 100gigaethernet 1/0/1 interface FEC enabled.

```
switch(config-100ge1/0/1)#fec mode rs
switch(config-100ge1/0/1)#
```

2.2.8 flow-statistic include-interframe

Function

The **flow-statistic include-interframe** command enables or disables interframe flow measurement.

Format

- **flow-statistic include-interframe** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the flow statistics function on the interface.	-
disable	Disables the flow statistics function on the interface.	-

Default Value

By default, the flow measurement function is disabled on an Ethernet interface.

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

None

Example

Enable the interframe flow measurement function on Ethernet interface 10gigaethernet 1/0/1.

```
switch(config-10ge1/0/1)#flow-statistic include-interframe enable
switch(config-10ge1/0/1)#
```

2.2.9 interface

Function

The **interface** command displays the interface configuration view. If the interface range is specified, the system enters the interface group configuration view.

Format

- **interface** { **10gigaethernet | 100gigaethernet** } *interface-number*
- **interface eth-trunk** *trunk-number*
- **interface** { **10gigaethernet** | **100gigaethernet** } *interface-number* **to** { **10gigaethernet** | **100gigaethernet** } *interface-number*

Parameters

Parameters	Description	Value
10gigaethernet	Specifies a 10Gigabit Ethernet interface.	-
100gigaethernet	Specifies a 100Gigabit Ethernet interface.	-
eth-trunk	Specifies a trunk interface.	-
interface-number	Specifies an Ethernet interface number.	The value is an integer string in the range of <1-1>/<0-2>/<1-52>.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 124.

Default Value

None

View

Global configuration view

Usage Guidelines

To set Parameters of an interface, you need to enter the interface configuration view using this command. If a trunk interface has no member interfaces, all commands are ineffective on the trunk interface.

Example

Enter the configuration view of Ethernet interfaces 10gigaethernet 1/0/1 to 10gigaethernet1/0/12.

```
switch(config)#interface 10gigaethernet 1/0/1 to 10gigaethernet 1/0/12
switch(config-10ge1/0/1->10ge1/0/12)#
```

2.2.10 interface loopback

Function

The **interface loopback** command enables the system to display the loopback interface view.
The **no interface loopback** command deletes a loopback interface view.

Format

- **interface loopback** *loopback-number*
- **no interface loopback** *loopback-number*

Parameters

Parameters	Description	Value
loopback-number	Specifies a loopback interface number.	The value is an integer in the range from 1 to 4.

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Enter the loopback1 configuration view.

```
switch(config)#interface loopback 1
switch(config-loopback-1)#
```

2.2.11mtu

Function

The **mtu** command sets the MTU for IPv4 interfaces on the switch.

Format

- **mtu** { *mtu* | **default** }

Parameters

Parameters	Description	Value
mtu-value	Specifies the MTU of interfaces.	The value is an integer ranging from 128 to 9216, in bytes.

Default Value

By default, the MTU of an interface is 1500 bytes.

View

Interface configuration view (10GE / 100GE / Trunk)

Usage Guidelines

You can use this command to set the MTU for interfaces on the switch.

Example

Set the MTU of Ethernet interface 10gigaethernet 1/0/1 to 1200.

```
switch(config)#interface loopback 1
switch(config-loopback-1)#
```

2.2.12 port-uniisolate

Function

The **port-uniisolate** command configures unidirectional port isolation.

Format

- **port-uniisolate interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **port-uniisolate interface eth-trunk** *trunk-number*
- **no port-uniisolate interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **no port-uniisolate interface eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of 1-1/0-2/1-52.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.

Default Value

None

View

Interface configuration view (Ethernet and trunk) and interface group configuration view

Usage Guidelines

None

Example

Configure unidirectional port isolation.

```
switch(config-10ge1/0/1)#port-uniisolate interface 10gigaethernet 1/0/2
switch(config-10ge1/0/1)#
```

2.2.13 port-down holdoff-timer

Function

The **port-down holdoff-timer** command configures the hold-off time for reporting the interface down event.

Format

- **port-down holdoff-timer** { *timer* | **default** }

Parameters

Parameters	Description	Value
timer	Specifies the holdoff time for reporting the interface down event.	The value is an integer ranging from 0 to 600000. The unit is millisecond.
default	Uses the default.	0 ms

Default Value

0 ms indicates that the interface down event is reported without delay.

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

When the device connected to the switch is switched over, the switch interface enters the Down state. You need to set the hold-off time for reporting the interface down event to avoid service interruption.

Example

Set the holdoff time for reporting the interface down event to 150 ms.

```
switch(config-10ge1/0/1)#port-down holdoff-timer 150
switch(config-10ge1/0/1)#
```

2.2.14 priority

Function

The **priority** command modifies the default priority of an interface.

Format

- **priority** *priority-level*

Parameters

Parameters	Description	Value
priority-level	port priority	The value is an integer in the range from 0 to 7.

Default Value

The default is 0.

View

Interface configuration view (10GE / 100GE / Trunk) and interface configuration view

Usage Guidelines

After the priority command is executed, you can set the default 802.1q priority for untagged packets received by the interface, that is, the priority value configured in this command.

Example

Set the priority of Ethernet interface 10gigaethernet 1/0/1 to 1.

```
switch(config-10ge1/0/1)#priority 1
switch(config-10ge1/0/1)#
```

2.2.15 rate-limit

Function

The **rate-limit** command sets the bandwidth of an interface.
The **no rate-limit** command cancels the bandwidth setting at an interface.

Format

- **rate-limit** { **in** | **out** } k**bps** k*bps*
- **rate-limit** { **in** | **out** } **mbps** *mbps*
- **rate-limit** { **in** | **out** } **percent** *percent*
- **no rate-limit** { **in** | **out** }

Parameters

Parameters	Description	Value
in	Sets the inbound bandwidth on the interface.	-
out	Sets the outbound bandwidth on the interface.	-
kbps	Sets the bandwidth rate.	The value is an integer ranging from 1 to 100000000.
mbps	Sets the bandwidth rate.	The value is an integer ranging from 1 to 100000.
percent	Sets the bandwidth percentage.	The value is an integer in the range from 1 to 100.

Default Value

None

View

Interface configuration view (10GE /100GE / Trunk)

Usage Guidelines

Some application scenarios require control of interface rates so as to provide different bandwidth for different users. Compared with the traffic policing feature in QoS application, bandwidth limiting at an interface can control the rate of all packets passing through the interface. If you only need to control the packet transmission and receiving rates at an interface and does not require rate limiting based on packet types, setting a bandwidth limit on the interface is a more convenient and simpler method.(N8550-32c and N8550-48B8C chips do not support inbound bandwidth.)

Example

Set the inbound bandwidth of Ethernet interface 10gigaethernet 1/0/1 to 2000mbps

```
switch(config-10ge1/0/1)#rate-limit in mbps 2000
switch(config-10ge1/0/1)#
```

2.2.16 reset counter

Function

The **reset counter** command resets packet counters at an interface.

Format

- **reset counter**

Parameters

None

Default Value

None

View

Interface configuration view (10GE / 100GE / Trunk) and interface group configuration view

Usage Guidelines

None

Example

Reset packet counters on interface 10gigaethernet 1/0/1.

```
switch(config-10ge1/0/1)#reset counter
switch(config-10ge1/0/1)#
```

2.2.17 show interface

Function

The **show interface** command displays attributes of an interface and related information.

Format

- **show interface**
- **show interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **show interface** { **10gigaethernet** | **100gigaethernet** } *interface-number* **config**
- **show interface eth-trunk** *trunk-number*
- **show interface eth-trunk** *trunk-number* **config**
- **show interface verbose**
- **show interface eth-trunk** *trunk-number* **verbose**
- **show interface eth-trunk** *trunk-number* **config**
- **show interface eth-trunk verbose**

Parameters

Parameters	Description	Value
10gigaethernet	Specifies a 10Gigabit Ethernet interface.	-
100gigaethernet	Specifies a 100Gigabit Ethernet interface.	-
eth-trunk	Specifies a trunk interface.	-
verbose	Displays information about all interfaces.	-
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of 1-1/0-2/1-52.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 124.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (10GE / 100GE / Trunk), interface group configuration view, Schedule-profile configuration view

Usage Guidelines

When checking interface attributes and related information:

- If you run **show interface** and do not specify the interface type and number, the command displays information about all Ethernet interfaces on the switch, including their interface numbers, status, whether they are bound to filters, their

inband IP addresses, and descriptions. If you specify the interface type and number in the command, the command displays information about the specified interface, including its duplex mode, rate, broadcast storm control function status, and packet statistics. If you specify **config** in the command, the displays other function configuration on the interface.

- If you run **show interface trunk** and do not specify the interface number, the command displays all the trunk interfaces that have been configured on the switch, the traffic distribution algorithms used on the trunk interfaces, and their member interface numbers. If the interface number is specified, the basic statistic information of a specified trunk interface will be displayed. If the Parameters config is specified, the pther function configuration of a specified trunk interface will be displayed.
- If you run **show interface verbose**, the command displays basic information about all Ethernet interfaces and trunk interfaces (if any) on the switch.

Generally, commands descried in this section are used to collect traffic statistics or diagnose faults on interfaces.

Example

Display the configuration of Ethernet interface 10gigaethernet 1/0/33.

```
switch#show interface 10gigaethernet 1/0/33
Interface 10gigaethernet1/0/33 admin state : up
 Line protocol current state : down
 The reason for down is up
 Switch Port, PVID : 1, The Maximum Frame Length is 9216
 IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 68:21:5f:fb:08:54
 Current system time: 2000-01-01 06:24:29
 Port Mode: optical
 Speed : 10000(Mbps),       Duplex: full,    Negotiation: disable
 Last 300 seconds input rate: 0 Bps, 0 pps, 0 bps
 Last 300 seconds output rate: 0 Bps, 0 pps, 0 bps
 Input peak rate 0/8 Bps, Record time: 2000-01-01 03:25:47
 Output peak rate 0/50 Bps, Record time: 2000-01-01 03:25:47
 Input:    0/101 packets,    0/15235 bytes
  Unicast              :              0/65           , Multicast              :              0/0
  Broadcast            :              0/36           , Jumbo                  :              0/0
  CRC                  :              0/0            , Giants                 :              0/0
  Jabbers              :              0/0            , Fragments              :              0/0
  Runs                 :              0/0            , DropEvents             :              0/0
  Alignments           :              0/0            , Symbols                :              0/0
  Ignoreds             :              0/0            , Frames                 :              0/0
  Discard              :              0/0            , Total Error            :              0/0
 Output:    0/3021 packets,    0/439928 bytes
  Unicast              :              0/1924         , Multicast              :              0/594
  Broadcast            :              0/503          , Jumbo                  :              0/0
  Collisions           :              0/0            , Deferreds              :              0/0
  Late Collisions :              0/0            , Excessive Collisions:              0/0
```

```
 Buffers Purged   :          0/0          , Discard          :          0/0
 Total Error      :          0/0
Input bandwidth utilization : 0.00%
Output bandwidth utilization : 0.00%
```

2.2.18 show interface statistic

Function

The **show interface statistic** command displays statistics at an interface.

Format

- **show interface statistic**
- **show interface statistic** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **show interface statistic brief**
- **show interface statistic brief** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **show interface statistic brief eth-trunk** *trunk-number*
- **show interface statistic eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer string in the range of <1-1>/<0-2>/<1-52>.
trunk-number	Specifies a trunk interface number.	The value is an integer ranging from 1 to 32.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (10GE / 100GE / Trunk), interface group configuration view

Usage Guidelines

Generally, commands descried in this section are used to collect traffic statistics or diagnose faults on interfaces.
If you do not specify an interface number when running this command, the command displays statistics about inbound and outbound packets on all the working interfaces on the switch in the order of interface numbers.
The command output information includes the following:

- Interface type and number
- Total number of packets sent or received by the interface
- Total number of unicast packets sent or received by the interface
- Total number of multicast packets sent or received by the interface
- Total number of broadcast packets sent or received by the interface
- Total number of error packets sent or received by the interface

Example

Display the statistics of Ethernet interface 10gigaethernet 1/0/1.

```
switch#show interface statistic
Interface          In(pkts) :Total          UniCast          MultiCast          BroadCast          Err
                     Out(pkts):Total          UniCast          MultiCast          BroadCast          Err
100ge1/0/1                  0/0              0/0              0/0              0/0              0/0
                            0/0              0/0              0/0              0/0              0/0
100ge1/0/2                  0/0              0/0              0/0              0/0              0/0
                            0/0              0/0              0/0              0/0              0/0
100ge1/0/3                  0/0              0/0              0/0              0/0              0/0
                            0/0              0/0              0/0              0/0              0/0
100ge1/0/4                  0/0              0/0              0/0              0/0              0/0
                            0/0              0/0              0/0              0/0              0/0
100ge1/0/5                  0/0              0/0              0/0              0/0              0/0
                            0/0              0/0              0/0              0/0              0/0
100ge1/0/6                  0/0              0/0              0/0              0/0              0/0
                            0/0              0/0              0/0              0/0              0/0
.....
```

2.2.19 show interface unit-number

Function

The **show interface unit-number** command shows the UNIT number of the device interface.

Format

- **show interface unit-number**

Parameters

None

Default Value

None

View

Common user view, privilege user view

Usage Guidelines

None

Example

Show the UNIT number of all interfaces.

```
switch#show interface unit-number
  Interface         Unit Number
  mgt-eth0/0/0      4097
  100ge1/0/1        4354
  100ge1/0/2        4355
  100ge1/0/3        4356
  100ge1/0/4        4357
  100ge1/0/5        4358
  100ge1/0/6        4359
  100ge1/0/7        4360
  100ge1/0/8        4361
  100ge1/0/9        4362
  100ge1/0/10       4363
  100ge1/0/11       4364
  100ge1/0/12       4365
  100ge1/0/13       4366
  100ge1/0/14       4367
  100ge1/0/15       4368
  100ge1/0/16       4369
  100ge1/0/17       4370
```

2.2.20 speed

Function

The **speed** command sets the speed of an Ethernet interface.(Only 100G port supports this command)

Format

- **speed** { **40000** | **100000** | **default** }

Parameters

Parameters	Description	Value
40000	Sets the interface rate to 40000 Mbit/s.	-
100000	Sets the interface rate to 100000 Mbit/s.	-
default	Sets the interface rate to the maximum rate supported by the interface.	-

Default Value

When an interface works in non-auto-negotiation mode, its default rate is the maximum rate supported by the interface.

View

Interface configuration view (Gigabit Ethernet), interface group configuration view (Gigabit)

Usage Guidelines

If two interconnected interfaces do not work at the same speed, use this command to change their rates to the same value so that the two interfaces can communicate normally.

Example

Set the speed of Ethernet interface 100gigaethernet 1/0/1 to 40000 Mbit/s.

```
switch(config-100ge1/0/1)#speed 40000
switch(config-100ge1/0/1)#
```

2.2.21 storm-control

Function

The **storm-control** command configures storm control for broadcast, multicast, and unicast packets on an Ethernet interface. The **no storm-control** command disables the storm control.

Format

- **storm-control** { **broadcast** | **multicast** | **dlf** } **percent** *value*
- **storm-control** { **broadcast** | **multicast** | **dlf** } cir { **kbps** | **Mbps** | **Gbps** } cir-*value*
- **no storm-control** { **broadcast** | **multicast** | **dlf** }

Parameters

Parameters	Description	Value
broadcast	Configures storm control for broadcast packets.	-
multicast	Configures storm control for multicast packets.	-
dlf	Configures storm control for unknown unicast packets.	-
value	Specifies the rate limit value in percentage.	The value is an integer in the range from 0 to 100.
cir-value	Specifies the rate limit value expressed in packet per second.	The value is an integer.Refer to actual equipment tips.

Default Value

By default, rates of broadcast, multicast, and unknown unicast packets are not limited at an interface.

View

Interface configuration view (10GE / 100GE / Trunk) and interface group configuration view

Usage Guidelines

To prevent waste of network resources, you can use this command to set a rate limit on broadcast, multicast, or unknown unicast packets based on actual situation of your network. The rate limit prevents such packets from consuming much bandwidth so that operation of user services can be guaranteed.

Note: The rate-limit and storm-control configurations can take effect simultaneously.

Example

Set a rate limit for broadcast packets on Ethernet interface 10gigaethernet 1/0/1.

```
switch(config-10ge1/0/1)#storm-control broadcast 64kbps 2
switch(config-10ge1/0/1)#
```

2.2.22 shutdown

Function

The **shutdown** command shuts down the current Ethernet interface.
The **no shutdown** command starts the current Ethernet interface.

Format

- **shutdown**
- **no shutdown**

Parameters

None

Default Value

By default, an Ethernet interface is in working state.

View

Interface configuration view (10GE / 100GE / Trunk), VLANIF configuration view, interface group configuration view, Tunnel interface configuration view

Usage Guidelines

If you modify the attributes of an interface but the new configuration does not take effect immediately, run the **shutdown** and **no shutdown** commands to shut down and then start the interface. The new configuration can then take effect.
If an interface is idle (with no cable connected), run the **shutdown** command to shut down the interface. This prevents exceptions caused by interference.
If you run the **shutdown** command in the trunk interface view, all member interfaces of the trunk interface will be shut down.

Warning: An interface must be started before configuration can be performed on it.If an interface is shut down during data transmission, data will be lost. Exercise caution when using this command.

Example

Shut down Ethernet interface 10gigaethernet 1/0/1.

```
switch(config-10ge1/0/1)#shutdown
switch(config-10ge1/0/1)#
```

2.2.23 switch {10gigaethernet|100gigaethernet}

Function

The **switch {10gigaethernet|100gigaethernet}** command is used to switch from one interface configuration view to another.

Format

- **switch** { **10gigaethernet** | **100gigaethernet** } *interface-number*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of 1-1/0-2/1-52.

Default Value

None

View

Interface configuration view (10GE / 100GE / Trunk) and interface group configuration view

Usage Guidelines

None

Example

Enter interface 10gigaethernet 1/0/12 from interface 10gigaethernet 1/0/1.

```
switch(config-10ge1/0/1)#switch 10gigaethernet 1/0/12
switch(config-10ge1/0/12)#
```

2.2.24 port flow-stat interval

Function

The**port flow-stat interval** command sets the time interval of traffic statistics for a port.

Format

- **port flow-stat interval** *interval*

Parameters

Parameters	Description	Value
interval	Specifies the time interval of traffic statistics for a port.	The value is an integer in the range from 30 to 300 (unit: s).

Default Value

0 second

View

Interface configuration view

Usage Guidelines

None

Example

Set the time interval of traffic statistics to 80s for a port.

```
switch(config-10ge1/0/1)#port flow-stat interval 80
switch(config-10ge1/0/1)#
```

2.2.25 flow-stat interval

Function

The**flow-stat interval** command sets the time interval of global traffic statistics.

Format

- **flow-stat interval** *interval*

Parameters

Parameters	Description	Value
interval	Specifies the time interval of global traffic statistics.	The value is an integer in the range from 30 to 300 (unit: s).

Default Value

300s

View

Global configuration view

Usage Guidelines

None

Example

Set the time interval of global traffic statistics to 300s.

```
switch(config)#flow-stat interval 300
switch(config)#
```

2.2.26 transceiver type

Function

The **transceiver type {1000BASE-X|1000BASE-T }** command configures the optical module type.

Format

- **transceiver type {1000BASE-X|1000BASE-T }**

Parameters

None

Default Value

1000BASE-X

View

Interface configuration view (10GE / 100GE) and interface group configuration view

Usage Guidelines

Refer to actual equipment tips.

Example

Configure the optical module type to 1000BASE-X.

```
switch(config-10ge1/0/1)#transceiver type 1000BASE-X
switch(config-10ge1/0/1)#
```

2.2.27 transceiver power low trigger error-down {enable|disable}

Function

The **transceiver power low trigger error-down {enable|disable}** command enables or disables an Ethernet optical interface to trigger the Error-Down function due to over-low Rx optical power.

Format

- **transceiver power low trigger error-down** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables an Ethernet optical interface to trigger the Error-Down function due to over-low Rx optical power.	-
disable	Disables an Ethernet optical interface to trigger the Error-Down function due to over-low Rx optical power.	-

Default Value

None

View

Interface configuration view (10GE / 100GE) and interface group configuration view

Usage Guidelines

Over-low optical power of the switch will lead to service interruption. To ensure the normal service running, the Error-down function is expected to be triggered if the optical power is over-low, so that services can be switched timely.

Example

Enable an Ethernet optical interface to trigger the Error-Down function due to over-low Rx optical power.

```
switch(config-10ge1/0/1)#transceiver power low trigger error-down enable
switch(config-10ge1/0/1)#
```

2.2.28 flush forward {enable|disable}

Function

The **flush forward {enable|disable}** command enables or disables the flush function at an interface.

Format

- **flush forward** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the flush function.	-
disable	Disables the flush function.	-

Default Value

By default, the flush function is disabled.

View

Interface configuration view (Ethernet and trunk) and interface group configuration view

Usage Guidelines

None

Example

Enable the flush function at an interface.

```
switch(config-10ge1/0/1)#flush forward enable
```

```
switch(config-10ge1/0/1)#
```

2.2.29 show flush

Function

The **show flush** command shows the global flush configuration.

Format

- **show flush**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

You can use this command to query the global flush configuration

Example

Show the global flush configuration.

```
switch#show flush
  Flush Max Interface Number      : 32
  Flush Free Interface Number     : 32
switch#
```

2.2.30 show flush interface

Function

The **show flush interface** command shows the flush interface configuration.

Format

- **show flush interface**

Parameters

None

Default Value

None

View

Privileged user view, global configuration view, common user view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

You can use this command to query the global flush interface configuration.

Example

Show the global flush interface configuration.

```
switch#show flush interface
Interface            FlushForward    LastFlushTime   RecPkt          SendPkt
10ge-1/0/1           disable         0               0               0
10ge-1/0/2           disable         0               0               0
10ge-1/0/3           disable         0               0               0
10ge-1/0/4           disable         0               0               0
10ge-1/0/5           disable         0               0               0
10ge-1/0/6           disable         0               0               0
10ge-1/0/7           disable         0               0               0
10ge-1/0/8           disable         0               0               0
10ge-1/0/9           disable         0               0               0
10ge-1/0/10          disable         0               0               0
10ge-1/0/11          disable         0               0               0
10ge-1/0/12          disable         0               0               0
10ge-1/0/13          disable         0               0               0
10ge-1/0/14          disable         0               0               0
10ge-1/0/15          disable         0               0               0
10ge-1/0/16          disable         0               0               0
10ge-1/0/17          disable         0               0               0
10ge-1/0/18          disable         0               0               0
10ge-1/0/19          disable         0               0               0
.....
```

2.2.31 show storm-control

Function

The **show storm-control interface** command displays the storm control information at an interface.
The **show storm-control vlan** command displays the storm control information on a VLAN interface.
The **show storm-control vsi** command displays the storm control information in a VSI instance.

Format

- **show storm-control interface**
- **show storm-control interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*

- **show storm-control vlan** [*vlan-id*]
- **show storm-control vsi** [*vsi-name*

Parameters

Parameters	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer in the range from 1 to 4094.
vsi-name	Specifies the name of a VSI instance to be displayed.	The value is a case-sensitive character string without spaces.
interface-number	Specifies an Ethernet interface number.	The value is an integer string in the range of <1-1>/<0-2>/<1-52>.

Default Value

None

View

Common user view, privileged user view, global configuration view, and VLANIF configuration view

Usage Guidelines

None

Example

Display the storm control information at an interface.

```
switch#show storm-control interface
Interface        Type          Status   Limit      Mode       CIR(kbit/s)     CBS(kbit)
10ge-1/0/33      multicast     enable   11100      pps        0               0
10ge-1/0/33      broadcast     disable  0          pps        0               0
10ge-1/0/33      dlf           disable  0          pps        0               0
switch#
```

2.3 MAC Address Table Configuration Commands

2.3.1 mac aging-time

Function

The **mac aging-time** command sets the aging time of dynamic MAC address entries.

Format

- **mac aging-time** { **0** | *aging-time* }

Parameters

Parameters	Description	Value

Parameters	Description	Value
aging-time	Specifies the aging time of dynamic MAC address entries.	The value is an integer. The values include 0 and 60 to 1000000 (unit: s).

Default Value

The default aging time of dynamic MAC address entries is 300 seconds.

View

Global configuration view

Usage Guidelines

If the aging time is set to 0, dynamic MAC address entries will not age out.
MAC address learning is a continuous dynamic process because the network topology keeps changing. To reduce the number of MAC address entries in the system, you can set an appropriate aging time for dynamic MAC address entries. This setting enables obsolete MAC address entries to be deleted in a timely manner.
The system starts an aging timer for each dynamic MAC address entry. A dynamic MAC address entry will be deleted if it is not updated within two times the aging time. If the MAC address entry is updated within this time period, the system resets its aging timer.

Note: Once the system is reset or the card is hot plugged or reset, dynamic entries are lost, but the stored static entries and blackhole entries are not aged or lost.

Example

Set the aging time of dynamic MAC address entries to 200 seconds.

```
switch(config)#mac aging-time 200
switch(config)#
```

2.3.2 mac-address static

Function

The **mac-address static** command creates a static MAC address entry.
The **no mac-addrss static** command deletes MAC address entries.

Format

- **mac-address static** *vlan-id mac-address* { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **mac-address static** *vlan-id mac-address* **eth-trunk** *trunk-number*
- **no mac-address static**
- **no mac-address static** *mac-address*
- **no mac-address static** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **no mac-address static** *vlan-id*
- **no mac-address static** *vlan-id mac-address*
- **no mac-address static eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
mac-address	Specifies the dynamic MAC address.	The value is in the format of AA:BB:CC:DD:EE:FF. In the MAC address, A, B, C, D, E, F are all hexadecimal numbers and can be 0, for example: 00:01:02:03:04:05. The MAC address cannot be set to FF:FF:FF:FF:FF:FF.
10gigaethernet	Specifies a 10Gigabit Ethernet interface.	-
100gigaethernet	Specifies a 100Gigabit Ethernet interface.	-
eth-trunk	Specifies a trunk interface.	-
interface-number	Specifies an Ethernet interface number.	The value is an integer string in the range of <1-1>/<0-2>/<1-52>.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.

Default Value

By default, no static MAC address entries are configured in the system.

View

Global configuration view

Usage Guidelines

None

Example

Create a static MAC address entry in VLAN 2, with destination MAC address 00:02:00:02:00:02, and outbound interface 10gigaethernet 1/0/1. That is, frames with destination MAC address 00:02:00:02:00:02 and belonging to VLAN 2 will be forwarded through outbound interface 10gigaethernet 1/0/1

```
switch(config)##mac-address static 2 00:02:00:02:00:02 10gigaethernet 1/0/1
switch(config)#
```

2.3.3 mac-address blackhole

Function

The **mac-address blackhole** command creates a blackhole MAC address entry.
The **no mac-address blackhole** command cancels the configuration.

Format

- **mac-address blackhole** *vlan-id mac-address*
- **no mac-address blackhole** *vlan-id mac-address*

Parameters

Parameters	Description	Value
vlan-id	Specifies the ID of the VLAN to which the outbound interface belongs.	The value is an integer in the range from 1 to 4094.
mac-address	Specifies the destination MAC address.	The value is in the AA:BB:CC:DD:EE:FF format, where each of the letters A to F represents a hexadecimal digit.

Default Value

By default, no blackhole MAC address entries are configured in the system.

View

Global configuration view

Usage Guidelines

Blackhole MAC address entries can prevent theft of data using embezzled user identities, enhancing system security.
After you create a blackhole MAC address entry using this command, any data frames with the specified MAC address as the source or destination MAC address will be discarded.

Example

Create a blackhole MAC address entry, with the destination MAC address 00:00:00:01:02:03 and outbound VLAN 10.

```
switch(config)#mac-address blackhole 10 00:00:00:01:02:03
switch(config)#
```

2.3.4 mac-learning {enable|disable}

Function

The **mac-learning {enable|disable}** command enables or disables MAC address learning at an interface.

Format

- **mac-learning** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables MAC address learning.	-
disable	Disables MAC address learning.	-

Default Value

By default, MAC address learning is enabled.

View

Interface configuration view (10GE / 100GE / Trunk) and interface group configuration view

Usage Guidelines

When the switch receives an Ethernet frame from another device, it obtains the source MAC address of the frame, binds the MAC address with the inbound interface of the frame, and adds this entry to the MAC address table. This process is called MAC address learning. After the new MAC address entry is learned, all the Ethernet frames destined for this MAC address are forwarded to the matching interface. This prevents broadcast of Ethernet frames.

Example

Disable MAC address learning on trunk 1.

```
switch(config-eth-trunk-1)#mac-learning disable
switch(config-eth-trunk-1)#
```

2.3.5 mac-address notification history-size

Function

The **mac-address notification history-size** command configures the size of the history of adding/deleting MAC addresses.

Format

- **mac-address notification history-size** { *history-size* | **default** }

Parameters

Parameters	Description	Value
history-size	Specifies the entry number of historical MAC address adding / deleting.	The value is an integer in the range from 1 to 128.
default	Uses the default.	64 second

Default Value

64 second

View

Global configuration view

Usage Guidelines

None

Example

Set the entry number of historical MAC address adding / deleting to 50.

```
switch(config)#mac-address notification history-size 50
switch(config)#
```

2.3.6 mac-learning disable action {forward|drop}

Function

The **mac-learning disable action {forward|drop}** command configures the action of a port after it is disabled with MAC address learning.

Format

- **mac-learning disable action** { **forward** | **drop** }

Parameters

Parameters	Description	Value
forward	Configures the action of a port to forwarding after it is disabled with MAC address learning.	-
drop	Configures the action of a port to dropping after it is disabled with MAC address learning.	-

Default Value

None

View

Interface configuration view (Ethernet and trunk), interface group configuration view

Usage Guidelines

None

Example

Configure the action of a port to dropping after it is disabled with MAC address learning.

```
switch(config-10ge1/0/1)#mac-learning disable action drop
switch(config-10ge1/0/1)#
```

2.3.7 mac-address notification {add|remove|all}

Function

The **mac-address notification {add|remove|all}** command enables the MAC address change notification for a port and configures the notification policy.
The **no mac-address notification** command disables the MAC address change notification for a port.

Format

- **mac-address notification** { **add** | **remove** | **all** }
- **no mac-address notification**

Parameters

Parameters	Description	Value
add	Sends notification when a MAC address is added.	-
remove	Sends notification when a MAC address is deleted.	-
all	Sends notification when a MAC address is added or deleted.	-

Default Value

By default, the MAC address change notification is disabled on a port.

View

Interface configuration view (Ethernet interface)

Usage Guidelines

You can use this command to enable the MAC address change notification for a port, so that the equipment can monitor the MAC address changing.

Example

Enable the MAC address change notification for a port and configures the notification policy.

```
switch(config-10ge1/0/1)#mac-address notification add
switch(config-10ge1/0/1)#
```

2.3.8 mac-address notification interval

Function

The **mac-address notification interval** command configures the interval of MAC address change notification.

Format

- **mac-address notification interval** { *interval-value* | **default** }

Parameters

Parameters	Description	Value
interval-value	Specifies the interval of MAC address change notification.	The value is an integer in the range from 10 to 1000 (unit: s).
default	Uses the default.	30 second

Default Value

30 second

View

Global configuration view

Usage Guidelines

If a port is enabled with MAC address notification, and it learns a new MAC address or a MAC address is removed from it, the change will be recorded and notified to Trap Server after the interval expires.

Example

Specify the interval of MAC address change notification to 60s.

2.3.9 mac-address flapping detection {enable|disable}

Function

The **mac-address flapping detection {enable|disable}** command enables or disables the global MAC address flapping detection.

Format

- **mac-address flapping detection** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the global MAC address flapping detection.	-
disable	Disables the global MAC address flapping detection.	-

Default Value

By default, the global MAC address flapping detection is enabled.

View

Global configuration view

Usage Guidelines

None

Example

Enable the global MAC address flapping detection.

```
switch(config)#mac-address flapping detection enable
switch(config)#
```

2.3.10 mac-address flapping aging-time

Function

The **mac-address flapping aging-time** command sets the aging time of MAC address flapping entries.

Format

- **mac-address flapping aging-time** { *aging-time* | **default** }

Parameters

Parameters	Description	Value
aging-time	Configures the aging time of MAC address flapping entries.	The value is an integer ranging from 60 to 900 in seconds.
default	Configures the default aging time of MAC address flapping entries.	300s

Default Value

300s

View

Interface configuration view, interface group configuration view

Usage Guidelines

None

Example

Configure the aging time of MAC address flapping entries.

```
switch(config-10ge1/0/1)#mac-address flapping aging-time 100
switch(config-10ge1/0/1)#
```

2.3.11mac-address flapping detection exclude-vlan

Function

The **mac-address flapping detection exclude-vlan** command configures the VLAN white list of MAC address flapping detection, that is, the VLANs not to be detected.

Format

- **mac-address flapping detection exclude-vlan** *vlan-id*

Parameters

Parameters	Description	Value

Parameters	Description	Value
vlan-id	Configures the VLAN white list of MAC address flapping detection.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Configure the VLAN white list of MAC address flapping detection to VLAN 100.

```
switch(config)#mac-address flapping detection exclude-vlan 100
switch(config)#
```

2.3.12 mac-address flapping detection vlan security-level

Function

The **mac-address flapping detection vlan security-level** command configures the security class of MAC address flapping detection in the VLAN.

Format

- **mac-address flapping detection vlan** *vlan-id* **security-level** { **high** | **middle** | **low** }

Parameters

Parameters	Description	Value
vlan-id	Configures the VLAN white list of MAC address flapping detection.	The value is an integer in the range from 1 to 4094.
high	Configures the security class of MAC address flapping detection in the specified VLAN to high. In this case, after three MAC address changes, the system ascertains that the MAC address flapping occurs.	-
middle	Configures the security class of MAC address flapping detection in the specified VLAN to middle. In this case, after ten MAC address changes, the system ascertains that the MAC address flapping occurs.	-
low	Configures the security class of MAC address flapping detection in the specified VLAN to low. In this case, after fifty MAC address changes, the system ascertains that the MAC address flapping	-

Parameters	Description	Value
	occurs.	

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Configure the security class of MAC address flapping detection in the VLAN to low.

```
switch(config)#mac-address flapping detection vlan 100 security-level low
switch(config)#
```

2.3.13 mac-address flapping quit-vlan recover-time

Function

The **mac-address flapping quit-vlan recover-time** command configures the automatic restoration time of a port after it exits a VLAN when MAC address flapping occurs on it.

Format

- **mac-address flapping quit-vlan recover-time** { *time* | **default** }

Parameters

Parameters	Description	Value
time	Specifies the automatic restoration time.	The value is an integer in the range from 0 to 1440.
default	Indicates the default automatic restoration time.	0 indicates no restoration. The default is 10 minutes.

Default Value

The default is 10.

View

Global configuration view

Usage Guidelines

None

Example

Configure the automatic restoration time of a port to 10 minutes after it exits a VLAN when MAC address flapping occurs on it.

```
switch(config)#mac-address flapping quit-vlan recover-time 10
switch(config)#
```

2.3.14 mac-address flapping action {quit-vlan|error-down}

Function

The **mac-address flapping action {quit-vlan|error-down}** command configures the action after MAC address flapping occurs for a port.
The **no mac-address flapping action** command disables the action.

Format

- **mac-address flapping action** { **quit-vlan** | **error-down** }
- **no mac-address flapping action**

Parameters

Parameters	Description	Value
quit-vlan	Configures a port to exit the VLAN after MAC address flapping occurs on it.	-
error-down	Shuts down a port after MAC address flapping occurs on it.	-

Default Value

None

View

Interface configuration view, interface group configuration view

Usage Guidelines

None

Example

Shut down a port after MAC address flapping occurs on it.

```
switch(config-10ge1/0/1)#mac-address flapping action error-down
switch(config-10ge1/0/1)#
```

2.3.15 mac-address flapping action priority

Function

The **mac-address flapping action priority** command configures the action priority after MAC address flapping occurs for a port.

Format

mac-address flapping action priority { *priority* | **default** }

Parameters

Parameters	Description	Value
priority	Configures the action priority after MAC address flapping occurs for a port.	The value is an integer in the range from 0 to 255.
default	Configures the default action priority for a port.	The default action priority is 127 for a port.

Default Value

127

View

Interface configuration view, interface group configuration view

Usage Guidelines

None

Example

Configure the action priority after MAC address flapping occurs to 127 for a port.

```
switch(config-10ge1/0/1)#mac-address flapping action priority 127
switch(config-10ge1/0/1)#
```

2.3.16 no mac-address

Function

The **no mac-address** command deletes MAC address entries learned globally or at an interface.

Format

- **no mac-address**
- **no mac-address** *mac-address*
- **no mac-address** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **no mac-address vlan** *vlan-id*
- **no mac-address vlan** *vlan-id mac-address*
- **no mac-address eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer string in the range of <1-1>/<0-2>/<1-52>.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 124.
mac-address	Specifies a MAC address.	The value is in the AA:BB:CC:DD:EE:FF format, where each of the letters A to F represents a hexadecimal digit.
vlan-id	Specifies a VLAN ID.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

Global configuration view and interface configuration view (Trunk)

Usage Guidelines

You can use this command to delete all MAC address entries learned on a specified interface.

Example

Delete all MAC address entries learned on interface 10gigaethernet 1/0/1.

```
switch(config-10ge1/0/1)#no mac-address
switch(config-10ge1/0/1)#
```

2.3.17 no mac-address {dynamic|static|security|sticky}

Function

The **no mac-address {dynamic|static|security|sticky}** command deletes all dynamic, static and security MAC address entries on the switch.

Format

- **no mac-address** { **dynamic** | **static** | **security** | **sticky** }
- **no mac-address** { **dynamic** | **static** | **security** | **sticky** } *mac-address*
- **no mac-address** { **dynamic** | **static** | **security** | **sticky** } *vlan-id*
- **no mac-address** { **dynamic** | **static** | **security** | **sticky** } *vlan-id mac-address*
- **no mac-address** { **dynamic** | **static** | **security** | **sticky** } { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **no mac-address** { **dynamic** | **static** | **security** | **sticky** } **eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value

Parameters	Description	Value
vlan-id	Specifies the VLAN interface ID.	The value is an integer in the range from 1 to 4094.
mac-address	Specifies the dynamic MAC address.	The value is in the AA:BB:CC:DD:EE:FF format, where each of the letters A to F represents a hexadecimal digit.
10gigaethernet	Specifies a 10Gigabit Ethernet interface.	-
100gigaethernet	Specifies a 100Gigabit Ethernet interface.	-
interface-number	Specifies an Ethernet interface number.	The value is an integer string in the range of <1-1>/<0-2>/<1-52>.
eth-trunk	Specifies a convergence interface.	-
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.

Default Value

None

View

Global configuration view and interface configuration view (Trunk)

Usage Guidelines

This command can delete global dynamic MAC address entries or specific dynamic MAC address entries according to the VLAN, VLAN+MAC address, MAC address, interface, or slot.

Example

Clear all dynamic MAC address entries.

```
switch(config)#no mac-address dynamic
switch(config)#
```

2.3.18 reset mac-address flapping record

Function

The **reset mac-address flapping record** command clears MAC address flapping record list.

Format

- **reset mac-address flapping record**

Parameters

None

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Clear the MAC address flapping record list.

```
switch(config)#reset mac-address flapping record
switch(config)#
```

2.3.19 reset mac-address notification history

Function

The **reset mac-address notification history** command clears the history of MAC address notification.

Format

- **reset mac-address notification history**

Parameters

None

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Clear the history of MAC address notification.

```
switch(config)#reset mac-address notification history
switch(config)#
```

2.3.20 show mac-address

Function

The **show mac-address** command displays MAC address entries.

Format

- **show mac-address** *mac-address*
- **show mac-address** *mac-address* **vlan** *vlan-id*
- **show mac-address** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **show mac-address eth-trunk** *trunk-number*
- **show mac-address vlan** *vlan-id*
- **show mac-address vsi** *vsi-name*
- **show mac-address** { **static** | **security** | **sticky** }
- **show mac-address** { **static** | **security** | **sticky** } { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **show mac-address** { **static** | **security** | **sticky** } **eth-trunk** *trunk-number*
- **show mac-address** { **static** | **security** | **sticky** } **vlan** *vlan-id*
- **show mac-address** { **static** | **security** | **sticky** } **vlan** *vlan-id* { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **show mac-address** { **static** | **security** | **sticky** } **vlan** *vlan-id* **eth-trunk** *trunk-number*
- **show mac-address** { **static** | **security** | **sticky** } **vsi** *vsi-name*

Parameters

Parameters	Description	Value
mac-address	Specifies a MAC address.	The value is in the AA:BB:CC:DD:EE:FF format, where each of the letters A to F represents a hexadecimal digit.
vlan-id	Specifies a VLAN ID.	The value is an integer in the range from 1 to 4094.
10gigaethernet	Specifies a 10Gigabit Ethernet interface.	-
100gigaethernet	Specifies a 100Gigabit Ethernet interface.	-
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of 1-1/0-2/1-52.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.
vsi-name	Specifies the name of a VSI instance to be displayed.	The value is a case-sensitive character string without spaces.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (10GE / 100GE / Trunk), interface group configuration view

Usage Guidelines

This command enables you to quickly find information about specific MAC address entries,
with a specified destination MAC address or those with a specified destination MAC address and a specified VLAN ID.

Example

Display information about MAC address entries.

```
switch#show mac-address vlan 1
  Total                :1
  Static               :0
  Dynamic              :1
  Blackhole            :0
  Sticky               :0
  Security             :0
  Snooping             :0

  MAC Address              Vlan/Vsi      Interface          Oper-Type             Type
  44:8a:5b:78:bf:7f    1/--              ge-1/0/8           forward               dynamic

switch#
```

2.3.21 show mac-address config

Function

The **show mac-address config** command displays the configuration of the MAC address table.

Format

- **show mac-address config**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, Interface configuration view (Trunk)

Usage Guidelines

None

Example

Display the configuration of the MAC address table.

```
switch#show mac-address config
 mac-address blackhole 10 00:00:00:00:00:01
switch#
```

2.3.22 show mac-address total-number

Function

The **show mac-address total-number** command displays the number of MAC addresses at an interface or VLAN.

Format

- **show mac-address total-number**
- **show mac-address total-number** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **show mac-address total-number eth-trunk** *trunk-number*
- **show mac-address total-number vlan** *vlan-id*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer string in the range of <1-1>/<0-2>/<1-52>.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.
vlan-id	Specifies the VLAN interface ID.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view, interface group configuration view

Usage Guidelines

None

Example

View the number of MAC address tables at interface ge1/0/1.

```
switch#show mac-address total-number
  Total       Static      Dynamic     Blackhole   Sticky      Security
  1           0           1           0           0           0
```

```
switch#
```

2.3.23 show mac-address blackhole

Function

The **show mac-address blackhole** command displays information about blackhole MAC address entries.

Format

- **show mac-address blackhole**
- **show mac-address blackhole vlan** *vlan-id*
- **show mac-address blackhole vsi** *vsi-name*

Parameters

Parameters	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer in the range from 1 to 4094.
vsi-name	Specifies the name of a VSI instance to be displayed.	The value is a case-sensitive character string without spaces.

Default Value

None

View

Common user view, privileged user view, global configuration view, Interface configuration view (Trunk)

Usage Guidelines

None

Example

Display information about blackhole MAC address entries.

```
switch#show mac-address blackhole
Blackhole      :1

 MAC Address       Vlan/Vsi   Interface      Oper-Type        Type
 00:00:00:00:00:11 1/--       N/A            discard          black-hole
```

2.3.24 show mac-address dynamic

Function

The **show mac-address dynamic** command displays information about dynamic MAC address entries.

Format

- **show mac-address dynamic**
- **show mac-address dynamic** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **show mac-address dynamic vlan** *vlan-id* { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **show mac-address dynamic vlan** *vlan-id* **eth-trunk** *trunk-number*
- **show mac-address dynamic eth-trunk** *trunk-number*
- **show mac-address dynamic vlan** *vlan-id*
- **show mac-address dynamic vsi** *vsi-name*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of 1-1/0-2/1-52.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.
vlan-id	Specifies a VLAN ID.	The value is an integer in the range from 1 to 4094.
vsi-name	Specifies the name of a VSI instance to be displayed.	The value is a case-sensitive character string without spaces.

Default Value

None

View

Common user view, privileged user view, global configuration view, Interface configuration view (Trunk)

Usage Guidelines

None

Example

Display information about dynamic MAC address entries at an interface.

```
switch#show mac-address dynamic

 Dynamic             :10

 MAC Address       Vlan/Vsi/BD Interface       Oper-Type        Type
 00:00:00:00:00:22 12/--/--    10ge1/0/34      forward          dynamic
 00:00:00:00:00:23 12/--/--    10ge1/0/34      forward          dynamic
 00:00:00:00:00:24 12/--/--    10ge1/0/34      forward          dynamic
 00:00:00:00:00:25 12/--/--    10ge1/0/34      forward          dynamic
 00:00:00:00:00:26 12/--/--    10ge1/0/34      forward          dynamic
 00:00:00:00:00:27 12/--/--    10ge1/0/34      forward          dynamic
 00:00:00:00:00:28 12/--/--    10ge1/0/34      forward          dynamic
```

```
 00:00:00:00:00:29   12/--/--    10ge1/0/34      forward          dynamic
 00:00:00:00:00:2a   12/--/--    10ge1/0/34      forward          dynamic
 00:00:00:00:00:2b   12/--/--    10ge1/0/34      forward          dynamic
switch#
```

2.3.25 show mac-address flapping record

Function

The **show mac-address flapping record** command displays the MAC address flapping history.

Format

- **show mac-address flapping record**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

None

Example

View the MAC address flapping history.

```
switch#show mac-address flapping record
 Move Time                Vlan  MAC Address       Original Port     Move Ports        Move Num
 S:2000-12-29 17:05:17    1     00:e0:4c:80:1a:50 10ge-1/0/47       10ge-1/0/27       1258
 E:2000-12-29 17:05:18
switch#
```

2.3.26 show mac-address notification history

Function

The **show mac-address notification history** command displays the history record of MAC address adding and deleting.

Format

- **show mac-address notification history**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

None

Example

```
# Show the history record of MAC address adding / deleting.
switch#show mac-address notification history
 History Index:1
 Timestamp:2000-12-29 17:02:24
 MAC Log Number:2
 ============================
 Time Stamp          Operation Vlan  MAC Address        Interface
 2000-12-29 17:02:24  flush     1    00:00:02:47:20:04  10ge-1/0/4
 2000-12-29 17:02:27  add       1    00:00:02:47:20:04  10ge-1/0/4
switch#
```

2.3.27 show mac info

Function

The **show mac info** command displays basic information about MAC addresses.

Format

- **show mac info**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, Interface configuration view (10GE / 100GE / Trunk)

Usage Guidelines

None

Example

Display basic information about MAC addresses.

```
switch#show mac info
  Aging time:300 seconds
switch#
```

2.3.28 show mac-address static

Function

The **show mac-address static** command displays information about static MAC address entries.

Format

- **show mac-address static**
- **show mac-address static** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **show mac-address static eth-trunk** *trunk-number*
- **show mac-address static vlan** *vlan-id*
- **show mac-address static vlan** *vlan-id* { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **show mac-address static vlan** *vlan-id* **eth-trunk** *trunk-number*
- **show mac-address static vsi** *vsi-name*

Parameters

Parameters	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer in the range from 1 to 4094.
10gigaethernet	Specifies a Gigabit Ethernet interface.	-
100gigaethernet	Specifies a 100Gigabit Ethernet interface.	-
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of 1-1/0-2/1-52.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.
vsi-name	Specifies the name of a VSI instance to be displayed.	The value is a case-sensitive character string without spaces.

Default Value

None

View

Common user view, privileged user view, global configuration view, Interface configuration view (Trunk)

Usage Guidelines

None

Example

Display information about static MAC address entries in all VLAN 1s.

```
switch#show mac-address static vlan 1
  MAC Address          Vlan/Vsi/BD   Interface        Oper-Type        Type
  00:00:00:00:00:02    1/--/--       100ge1/0/1       forward          static
```

2.4 ARP Configuration Commands

2.4.1 arp detect-mode unicast

Function

The **arp detect-mode unicast** command enables or disables the ARP aging unicast detection.

Format

- **arp detect-mode unicast** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables ARP aging unicast detection.	-
disable	Disables ARP aging unicast detection.	-

Default Value

By default, ARP aging unicast detection is disabled.

View

Interface configuration view (Ethernet), VLAN configuration view, interface group configuration view, global configuration view

Usage Guidelines

None

Example

Enable ARP aging unicast detection.

```
switch(config-10ge1/0/1)#arp detect-mode unicast enable
switch(config-10ge1/0/1)#
```

2.4.2 arp learning dhcp-trigger {enable|disable}

Function

The **arp learning dhcp-trigger {enable|disable}** command enables or disables DHCP-triggered ARP learning.

Format

- **arp learning dhcp-trigger** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables DHCP-triggered ARP learning.	-
disable	Disables DHCP-triggered ARP learning.	-

Default Value

None

View

VLANIF configuration view

Usage Guidelines

None

Example

Enable DHCP-triggered ARP learning.

```
switch(config-vlanif-100)#arp learning dhcp-trigger enable
switch(config-vlanif-100)#
```

2.4.3 ip arp

Function

The **ip arp** command creates a static ARP entry on an Ethernet interface or trunk interface.
The **no ip arp** command deletes a static ARP entry.

Format

- **ip arp** *ip-address mac-address* { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **ip arp** *ip-address mac-address* **eth-trunk** *trunk-number*
- **no ip arp** *ip-address*

Parameters

Parameters	Description	Value
ip-address	Specifies the IP address in the static ARP entry.	The value is in dotted decimal notation.
mac-address	Specifies the MAC address in the static ARP entry.	The value is in the AA:BB:CC:DD:EE:FF format, where each of the letters A to F represents a hexadecimal digit.
interface-number	Specifies the Ethernet interface number in the static ARP entry.	The value is an integer in the range of 1-1/0-2/1-52.
trunk-number	Specifies the trunk interface number in the static ARP entry.	The value is an integer ranging from 1 to 32.

Default Value

By default, the system has no ARP entries and learns MAC and IP address mappings through dynamic ARP.

View

Global configuration view

Usage Guidelines

Static ARP entries can only be deleted manually, and will not be aged out or updated dynamically. These static ARP entries are always effective during normal operation of the switch.
The IP address specified in a static ARP entry must be on the same network segment as the local IP address in the VLAN and cannot be the same as the local IP address.
The interface specified by *trunk-number* must be added to the VLAN on the same network segment as the IP address in the static ARP entry.

Note: The ip-address specified in the command must be on the same network segment as the IP address of the interface specified by interface-number.
ARP entries apply only to local area networks.
Currently, the switch does not support static ARP entry configuration on member interfaces of a trunk interface.

Example

Create an ARP entry, in which the IP address is 10.18.2.123, the MAC address is 00:00:02:00:00:01, and interface is 10gigaethernet 1/0/1.

```
switch(config)#ip arp 10.18.2.123 00:00:02:00:00:01 10gigaethernet 1/0/1
switch(config)#
```

2.4.4 ip arp detect {enable|disable}

Function

The **ip arp detect {enable|disable}** command configures ARP automatic detection and learning.

Format

- **ip arp detect** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables ARP automatic detection and learning.	-
disable	Disables ARP automatic detection and learning.	-

Default Value

By default, ARP automatic detection and learning is enabled.

View

Global configuration view

Usage Guidelines

None

Example

Disable ARP automatic detection and learning.

```
switch(config)#ip arp detect disable
switch(config)#
```

2.4.5 ip arp detect-times

Function

The **ip arp detect-times** command configures the number of aging detection times for dynamic ARP entries.

Format

- **ip arp detect-times** { *times-num* | **default** }

Parameters

Parameters	Description	Value
times-num	Specifies the number of aging detection times for dynamic ARP entries.	The value is an integer in the range from 0 to 10.
default	Specifies the default number of aging detection times for dynamic ARP entries.	3

Default Value

By default, the number of aging detection times for dynamic ARP entries is 3.

View

Global configuration view

Usage Guidelines

None

Example

Set the number of aging detection times for dynamic ARP entries to 5.

```
switch(config)#ip arp detect-times 5
switch(config)#
```

2.4.6 ip arp aging-time

Function

The **ip arp aging-time** command sets the aging time of dynamic ARP entries.
The **no ip arp aging-time** command restores the aging time of dynamic ARP entries to the default.

Format

- **ip arp aging-time** { *aging-time* | **default** }

Parameters

Parameters	Description	Value
aging-time	Specifies the aging time of dynamic ARP entries.	The value is an integer in the range from 60 to 1200 (unit: s).
default	default	1200s

Default Value

The default aging time of dynamic ARP entries is 1200 seconds.

View

Global configuration view

Usage Guidelines

Setting an appropriate aging time of dynamic ARP entries can reduce the address resolution errors caused by slow updates of dynamic ARP entries.

Example

Set the aging time of dynamic ARP entries to 300 seconds.

```
switch(config)#ip arp aging-time 300
switch(config)#
```

2.4.7 flush arp

Function

The **flush arp** command deletes static, dynamic or all the ARP entries.

Format

- **flush arp** { **all** | **dynamic** | **static** }

Parameters

Parameters	Description	Value
all	Deletes all static and dynamic ARP entries.	-
dynamic	Deletes all dynamic ARP entries.	-
static	Deletes all static ARP entries.	-

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to manually delete all dynamic ARP entries if needed.
This command cancels mappings between IP and MAC addresses, which may lead to temporary access failures to some nodes. Therefore, exercise caution when using this command.

Example

Delete all dynamic ARP entries.

```
switch(config)#flush arp all
switch(config)#
```

2.4.8 show arp-probe database

Function

The **show arp-probe database** command shows major content of all ARP entries notified by the kernal or obtained through active/standby synchronization.

Format

- **show arp-probe database**

- **show arp-probe database dst-ip** *dst-ip*
- **show arp-probe database dst-ip6** *dst-ip6*

Parameters

Parameters	Description	Value
dst-ip	Specifies the destination IP address.	The value is in dotted decimal notation
dst-ip6	Specifies the destination IPv6 address.	A 128-bit IPv6 address is divided into 8 groups, with 16 bits in each group. Each group is expressed by four hexadecimal digits (0-9 and A-F), and two groups are separated with a colon (:). Each X represents a group of hexadecimal digits.

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view

Usage Guidelines

You can use this command to view all ARP entry information notified by the kernal or obtained through active/standby synchronization.

Example

Display major content of all entries.

```
switch#show arp-probe database
  Dst-ip                Mac                Interface      Port           State
  10.32.133.31          30:0D:9E:84:C2:EC mgt-eth0/0/0   mgt-eth0/0/0   incomplete
  10.32.133.192         68:21:5F:DB:FC:00 mgt-eth0/0/0   mgt-eth0/0/0   incomplete
  10.32.133.193         68:21:5F:DC:0B:00 mgt-eth0/0/0   mgt-eth0/0/0   incomplete
  10.32.133.195         68:21:5F:FB:08:54 mgt-eth0/0/0   mgt-eth0/0/0   incomplete
  10.32.133.254         78:2C:29:4B:A2:01 mgt-eth0/0/0   mgt-eth0/0/0   incomplete
switch#
```

2.4.9 show arp-probe database verbose

Function

The **show arp-probe database verbose** command shows all content of all ARP entries notified by the kernal or obtained through active/standby synchronization.

Format

- **show arp-probe database verbose**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view

Usage Guidelines

None

Example

Display all content of all entries.

```
switch#show arp-probe database verbose
  Destination Ip Address                : 10.32.133.31
 Mac Address                            : 30:0D:9E:84:C2:EC
 Interface                              : mgt-eth0/0/0
 Out Port                               : mgt-eth0/0/0
 State                                  : incomplete
 Send Time                              : 2 days 1 hours 15 minutes 1 seconds
 VPN Instance                           : public
 Destination Ip Address                 : 10.32.133.192
 Mac Address                            : 68:21:5F:DB:FC:00
 Interface                              : mgt-eth0/0/0
 Out Port                               : mgt-eth0/0/0
 State                                  : incomplete
 Send Time                              : 2 days 1 hours 15 minutes 1 seconds
 VPN Instance                           : public
 Destination Ip Address                 : 10.32.133.193
 Mac Address                            : 68:21:5F:DC:0B:00
 Interface                              : mgt-eth0/0/0
 Out Port                               : mgt-eth0/0/0
 State                                  : incomplete
 Send Time                              : 2 days 1 hours 15 minutes 1 seconds
 VPN Instance                           : public
 Destination Ip Address                 : 10.32.133.195
 Mac Address                            : 68:21:5F:FB:08:54
 Interface                              : mgt-eth0/0/0
```

```
Out Port                    : mgt-eth0/0/0
State                       : incomplete
Send Time                   : 2 days 1 hours 15 minutes 1 seconds
VPN Instance                : public
Destination Ip Address      : 10.32.133.254
Mac Address                 : 78:2C:29:4B:A2:01
Interface                   : mgt-eth0/0/0
Out Port                    : mgt-eth0/0/0
State                       : incomplete
Send Time                   : 2 days 1 hours 15 minutes 1 seconds
VPN Instance                : public
```

2.4.10 show arp-probe global

Function

The **show arp-probe global** command shows global information and related statistics.

Format

- **show arp-probe global**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view

Usage Guidelines

None

Example

Display global information and relevant statistics.

```
switch#show arp-probe global
Version                 : ARPPROBE_VL3.00.00.00
Max ARP Num             : 4096
Current ARP Num         : 21
Max Interface Num       : 332
Current Interface Num   : 0
```

```
Synchronous Add Num            : 0
Synchronous Add Failed Num : 0
Synchronous Del Num            : 0
Synchronous Del Failed Num : 0
Synchronous Recv Add Num    : 0
Synchronous Recv Add Failed Num : 0
Synchronous Recv Del Num    : 0
Synchronous Recv Del Failed Num : 0
Pkt Send Num                       : 846
Pkt Send Failed Num            : 0
Sys Recv Add Num                : 28
Sys Recv Add Failed Num     : 0
Sys Recv Del Num                : 7
Sys Recv Del Failed Num     : 0
Sys Add Num                        : 0
Sys Add Failed Num             : 0
Sys Del Num                        : 0
Sys Del Failed Num             : 0
switch#
```

2.4.11show ip arp

Function

The **show ip arp** command displays ARP information matching the specified condition.

Format

- **show ip arp**
- **show ip arp** *ip-address*
- **show ip arp dynamic**
- **show ip arp static**
- **show ip arp** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **show ip arp eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer in the range from 1 to 4094.
10gigaethernet	Specifies a 10Gigabit Ethernet interface.	-
100gigaethernet	Specifies a 100Gigabit Ethernet interface.	-
interface-number	Specifies the Ethernet interface number in the static ARP entry.	The value is an integer in the range of 1-1/0-2/1-52.

Parameters	Description	Value
trunk-number	Specifies the trunk interface number in the static ARP entry.	The value is an integer ranging from 1 to 32.
string	Specifies a character string used for filtering the information to be displayed.	The value is a character string.

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Display ARP information on the switch.

```
switch#show ip arp
  Arp aging time: 1200(s)
  Destination      Mac-addr            Type      Aging     Vlan     Interface          Vpn-instance
  ------------------------------------------------------------------------------------------------
  10.32.133.45     00d0:f822:3347      dynamic   945       N/A      mgt-eth0/0/0
  10.32.133.46     ccef:4812:d5bf      dynamic   945       N/A      mgt-eth0/0/0
  10.32.133.195    6821:5ffb:0854      if        never     4097     mgt-eth0/0/0
  10.32.133.254    782c:294b:a201      dynamic   1199      N/A      mgt-eth0/0/0
  ------------------------------------------------------------------------------------------------
  Total: 4          Dynamic: 3          Static: 0          Other: 1
```

2.5 ARP Proxy

2.5.1 debug arp-proxy

Function

The debug **ARP-Proxy** command can be used to turn on the proxy ARP synchronous debugging function.
The no **Debug arp-Proxy** command can be used to turn off Proxy ARP synchronous debugging capabilities.

Format

- **debug arp-proxy**
- **no debug arp-proxy**

Parameters

None

Default Value

By default, ARP-Proxy debugging is turned off.

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Turn off Proxy ARP debugging.

```
switch#no debug arp-proxy
switch#
```

2.5.2 arp-proxy {enable|disable}

Function

Arp-proxy {enable|disable} can be used to enable or disable the routed proxy arp functionality of the VLANIF interface.

Format

- **arp-proxy** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Routed proxy ARP is enabled on the VLANIF interface.	-
disable	Routed proxy ARP is disabled on the VLANIF interface.	-

Default Value

By default, routed proxy ARP is disabled on an interface.

View

VLANIF interface view

Usage Guidelines

When two hosts reside on different network segments and do not have default gateways configured, run the arp proxy enable command on the device that connects to the two hosts to enable routed proxy ARP. This configuration implements IP address resolution between the two hosts.The network IDs in the IP addresses of hosts on each subnet must be the same.

Example

Routed proxy ARP is enabled on the VLANIF interface

```
switch(config-vlanif-2)#arp-proxy enable
switch(config-vlanif-2)#
```

2.5.3 arp-proxy inner-sub-vlan-proxy {enable|disable}

Function

arp-proxy inner-sub-vlan-proxy {enable|disable} command enables or disables inner-VLAN proxy Address Resolution Protocol (ARP).

Format

- **arp-proxy inner-sub-vlan-proxy** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Inner-VLAN proxy ARP is enabled.	-
disable	Inner-VLAN proxy ARP is disabled.	-

Default Value

By default, inner-VLAN proxy ARP is disabled

View

VLANIF interface view

Usage Guidelines

None

Example

Inner-VLAN proxy ARP is enabled.

```
switch(config-vlanif-2)#arp-proxy inner-sub-vlan-proxy enable
switch(config-vlanif-2)#
```

2.5.4 arp-proxy inter-sub-vlan-proxy {enable|disable}

Function

arp-proxy inter-sub-vlan-proxy {enable|disable} command enables or disables inter-VLAN proxy Address Resolution Protocol (ARP).

Format

- **arp-proxy inter-sub-vlan-proxy** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Inter-VLAN proxy ARP is enabled.	-
disable	Inter-VLAN proxy ARP is disabled.	-

Default Value

By default, inter-VLAN proxy ARP is disabled.

View

VLANIF interface view

Usage Guidelines

None

Example

Inter-VLAN proxy ARP is enabled.

```
switch(config-vlanif-2)#arp-proxy inter-sub-vlan-proxy enable
switch(config-vlanif-2)#
```

2.5.5 show arp-proxy config

Function

show arp-proxy config command can be used to display configuration information for ARP-Proxy.

Format

- **show arp-proxy config**

Parameters

None

Default Value

None

View

Common user view,VLANIF configuration view,privileged user view and global configuration view

Usage Guidelines

None

Example

Display ARP-proxy information on the switch.

```
switch#show arp-proxy config
interface vlan 2
arp-proxy enable
arp-proxy inner-sub-vlan-proxy enable
switch#
```

2.5.6 show arp-proxy vlan

Function

show arp-proxy vlan command can be used to display AR-Proxy VLAN information.

Format

- **show arp-proxy vlan**

Parameters

None

Default Value

None

View

Common user view,VLANIF configuration view,privileged user view and global configuration view

Usage Guidelines

None

Example

Display ARP-proxy vlan information on the switch.

```
Switch(config)#show arp-proxy vlan
 Vlan ArpProxy   InnerSubVlanProxy     InterSubVlanProxy
   1     disable      disable                  disable
   2     enable       enable                   disable
Switch(config)#
```

2.6 Link Aggregation Configuration Commands

2.6.1 active-linknumber

Function

The **active-linknumber** command sets the maximum and minimum numbers of active member interfaces in a link aggregation group.

Format

- **active-linknumber min** { *min-number* | **default** }
- **active-linknumber max** { *max-number* | **default** }

Parameters

Parameters	Description	Value
{ min-number | default }	Specifies the minimum number of active member interfaces.	The value of *min-number* is an integer ranging from 1 to 8. If default is specified, the value is 1.
{ max-number | default }	Specifies the maximum number of active member interfaces.	The value of *max-number* is an integer ranging from 1 to 8. If default is specified, the value is 8.

Default Value

By default, the minimum number of active interfaces in a link aggregation interface is 1 and the maximum number of active interfaces is 8.

View

Trunk interface configuration view

Usage Guidelines

The number of active member links in a link aggregation group (trunk interface) affects the state and bandwidth of the trunk interface. To ensure stability of the trunk interface, set the minimum or maximum number of active member interfaces, thereby reducing the impact of member link state changes on the trunk interface.

- If the number of member links in Up state is smaller than the minimum number, the trunk interface state changes to Down. Setting the minimum value of active links ensures the minimum bandwidth of the trunk interface.
- If the number of member links in Up state reaches the maximum value, the bandwidth of the trunk interface will not increase after more member links change to Up state. Setting the maximum number of active links improves network reliability while ensuring sufficient bandwidth on the trunk interface.

The minimum number of active member interfaces must be smaller than the maximum number of active member interfaces that has been configured for the trunk interface.

If the minimum or maximum number of active member interfaces is configured multiple times, the last configuration takes effect.

Example

On trunk 1, set the maximum number of active member interfaces to 6 and the minimum number of active member interfaces to 2.

```
switch(config-eth-trunk-1)#active-linknumber max 6
switch(config-eth-trunk-1)#

switch(config-eth-trunk-1)#active-linknumber min 2
switch(config-eth-trunk-1)#
```

2.6.2 add

Function

The **add** command adds a member interface in the trunk interface configuration view.

Format

- **add** { **10gigaethernet** | **100gigaethernet** } *interface-number*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of 1-1/0-2/1-52.

Default Value

By default, a trunk interface has no member interfaces.

View

Trunk interface configuration view

Usage Guidelines

You can use this command to bind multiple physical interfaces into a logical interface (trunk interface). Each physical interface is called a member interface. Link aggregation technology (trunk) can increase link bandwidth, enhance link reliability, and implement load balancing.
Before using this command, run the **interface trunk** command to create a trunk interface first.
The switch supports cross-card trunk interfaces. That is, interfaces on different cards can be bound as one trunk interface.
The switch supports a maximum of 124 trunk interfaces and allows each trunk interface to have a maximum of 8 member interfaces. Member interfaces of the same trunk interface must have the same settings of the following attributes. Otherwise, they cannot be bound to the same trunk interface.

- Link type
- Speed
- Duplex mode
- Flow control mode

You are also advised to use the same settings for other interface attributes, including but not limited to:

Rate limits for broadcast, multicast, and unknown unicast packets for storm control
Dropping of broadcast, multicast, and unknown unicast packets for storm control

- VLAN ID of the interfaces
- VLAN mapping
- QinQ
- Interface priority
- Whether to allow BPDU packets to pass
- MAC address learning
- Static multicast group membership

Attributes of member interfaces cannot be changed individually. You can only change the attributes of the trunk interface, which will change the corresponding attributes of all member interfaces.
To ensure normal communication between the devices connected by a trunk link, you must ensure consistent settings of the following physical attributes on both ends in addition to consistent physical attribute settings of trunk member interfaces:

- Number of physical interfaces connected on the two ends
- Rate of physical interfaces connected on the two ends
- Duplex mode of physical interfaces connected on the two ends
- Flow control mode of physical interfaces connected on the two ends

Example

Add member interface 10gigaethernet1/0/1 to trunk 1.

```
switch(config-eth-trunk-1)#add 10gigaethernet 1/0/1
switch(config-eth-trunk-1)#
```

2.6.3 interface eth-trunk

Function

The **interface eth-trunk** command creates a trunk interface and displays the trunk interface configuration view.
The **no interface eth-trunk** command deletes an existing trunk interface.

Format

- **interface eth-trunk** *trunk-number*
- **no interface eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.

Default Value

None

View

Global configuration view

Usage Guidelines

If the specified trunk interface has been created, this command displays the trunk interface configuration view directly.
When you use the **no** form of the command to delete an existing trunk interface, the system first deletes member interfaces of the trunk interface. You do not need to delete the member interfaces manually.

Example

Create trunk 1 and display its configuration view.

```
switch(config)#interface eth-trunk 1
switch(config-eth-trunk-1)#
```

2.6.4 join eth-trunk

Function

The **join eth-trunk** command adds an interface to a specified trunk interface.
The **no join eth-trunk** command deletes an interface from a specified trunk interface.

Format

- **join eth-trunk** *trunk-number*
- **no join eth-trunk**

Parameters

Parameters	Description	Value
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.

Default Value

By default, an Ethernet interface does not belong to any trunk interface.

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

You can use this command to bind multiple physical interfaces into a logical interface (trunk interface). Each physical interface is called a member interface. Link aggregation technology (trunk) can increase link bandwidth, enhance link reliability, and implement load balancing.
Before using this command, run the **interface trunk** command to create a trunk interface first.
The switch supports cross-card trunk interfaces. That is, interfaces on different cards can be bound as one trunk interface.
The switch supports a maximum of 124 trunk interfaces and allows each trunk interface to have a maximum of 8 member interfaces. Member interfaces of the same trunk interface must have the same settings of the following attributes. Otherwise, they cannot be bound to the same trunk interface.

- Link type
- Speed

- Duplex mode
- Flow control mode

You are also advised to use the same settings for other interface attributes, including but not limited to:

Rate limits for broadcast, multicast, and unknown unicast packets for storm control

Dropping of broadcast, multicast, and unknown unicast packets for storm control

- VLAN ID of the interfaces
- VLAN mapping
- QinQ
- Interface priority
- Whether to allow BPDU packets to pass
- MAC address learning
- Static multicast group membership

Attributes of member interfaces cannot be changed individually. You can only change the attributes of the trunk interface, which will change the corresponding attributes of all member interfaces.

To ensure normal communication between the devices connected by a trunk link, you must ensure consistent settings of the following physical attributes on both ends in addition to consistent physical attribute settings of trunk member interfaces:

- Number of physical interfaces connected on the two ends
- Rate of physical interfaces connected on the two ends
- Duplex mode of physical interfaces connected on the two ends
- Flow control mode of physical interfaces connected on the two ends

Example

Enter the configuration view of interface 10gigaethernet1/0/3 and add it to trunk 1.

```
switch(config-10ge1/0/3)#join eth-trunk 1
  %Join eth-trunk 1 successfully.
switch(config-10ge1/0/3)#
```

2.6.5 lacp system-priority

Function

The **lacp system-priority** command sets the LACP system priority.

Format

- **lacp system-priority** { *priority* | **default** }

Parameters

Parameters	Description	Value
priority	Specifies the LACP system priority.	The value is an integer in the range from 0 to 65535.
default	Uses the default priority value.	32768

Default Value

32768

View

Global configuration view

Usage Guidelines

None

Example

Set the LACP system priority to 100.

```
switch(config)#lacp system-priority 100
switch(config)#
```

2.6.6 load-balance

Function

The **load-balance** command sets the load balancing mode for trunk interfaces.

Format

- **load-balance schedule-profile** *profile-name*
- **load-balance** { **src-mac** | **dst-mac** | **srcdst-mac** | **src-ip** | **dst-ip** | **srcdst-ip** | **default** }

Parameters

Parameters	Description	Value
profile-name	Specifies the profile name of enhanced load sharing applied to the trunk interface, valid to all trunk interfaces	The value is a string of 1 to 33 characters.
src-mac	Specifies load balancing among trunk member interfaces based on source MAC addresses, valid to all trunk interfaces.	-
dst-mac	Specifies load balancing among trunk member interfaces based on destination MAC addresses, valid to all trunk interfaces.	-
srcdst-mac	Specifies the exclusive OR or load balancing among trunk member interfaces based on source and destination MAC addresses, valid to all trunk interfaces.	-
src-ip	Specifies load balancing among trunk member interfaces based on source IP addresses, valid to all trunk interfaces.	-
dst-ip	Specifies load balancing among trunk member interfaces based on destination IP addresses, valid to all trunk interfaces.	-
srcdst-ip	Specifies the exclusive OR or load balancing among trunk member interfaces based on source and destination IP addresses, valid to all trunk interfaces.	

Default Value

srcdst-mac

View

Global configuration view

Usage Guidelines

This command enables data traffic to be distributed on different member links properly and finally reach the same destination, preventing link congestion. Choose an appropriate load balancing mode based on actual situation on your network. Generally, load balancing based on more frequently changing variables can ensure more balanced traffic distribution on member links.
The traffic distribution algorithm configured in global configuration mode is valid to all trunk interfaces.
Load balancing applies only to outbound traffic; therefore, different load balancing modes can be set on two ends of the trunk link.
If you run this command multiple times, the last configured load balancing mode takes effect.

Example

Configure global load balancing based on destination IP addresses.

```
switch(config-eth-trunk1)#load-balance dst-ip
switch(config-eth-trunk1)#
```

2.6.7 ip field

Function

The **ip field** command configures the load balancing mode of IPv4 packets in the enhanced load balancing template.
The **no ip field** command deletes the configured load balancing mode of IPv4 packets in the enhanced load balancing template.

Format

- **ipv4 field** { **src-ip** | **dst-ip** | **l4-srcport** | **l4-dstport** | **all** | **default** }
- **no ipv4 field** { **src-ip** | **dst-ip** | **l4-srcport** | **l4-dstport** }

Parameters

Parameters	Description	Value
src-ip	Specifies load balancing based on the source IPv4 address.	-
dst-ip	Specifies load balancing based on the destination IPv4 address.	-

Parameters	Description	Value
l4-srcport	Specifies load balancing based on the source port on the transport layer.	-
l4-dstport	Specifies load balancing based on the destination port on the transport layer.	-
all	Specifies load balancing based on all of the preceding fields.	-
default	Specifies load balancing based on the source IP address and destination IP address by default.	-

Default Value

By default, the load balance mode of IPv4 packets is set to src-ip and dst-ip.

View

Schedule-profile configuration view

Usage Guidelines

None

Example

Set the load balancing mode of IPv4 packets in the enhanced load balancing template 123 to src-ip.

```
switch(config-schedule-profile-123)#ip field src-ip
switch(config-schedule-profile-123)#
```

2.6.8 ipv6 field

Function

The **ipv6 field** command configures the load balancing mode of IPv6 packets in the enhanced load balancing template.
The **no ipv6 field** command deletes the load balancing mode of IPv6 packets in the enhanced load balancing template.

Format

- **ipv6 field** { **src-ip** | **dst-ip** | **l4-srcport** | **l4-dstport** | **all** | **default** }
- **no ipv6 field** { **src-ip** | **dst-ip** | **l4-srcport** | **l4-dstport** }

Parameters

Parameters	Description	Value
src-ip	Specifies the source IP address of IPv6 packets as the basis of load balancing.	-
dst-ip	Specifies the destination IP address of IPv6 packets as the basis of load balancing.	-
l4-srcport	Specifies load balancing based on the source port on the IPv6 transport layer.	-

Parameters	Description	Value
l4-dstport	Specifies load balancing based on the destination port on the IPv6 transport layer.	-
default	Restores default settings.	-
all	Specifies load balancing based on all of the preceding IPv6 fields.	-

Default Value

By default, the load balancing mode of IPv6 packets is set to src-ip and dst-ip.

View

schedule-profile configuration view

Usage Guidelines

After trunk technology is used, multiple physical links exist between two devices. If the first data frame is transmitted on the first link and the second data frame is transmitted on the second link, the second data frame may arrive the opposite end equipment first. To prevent the out-of-sequence, the load balancing mode is suggested. Load balancing ensures that the data frames belonging to one data stream arrive at the destination in sequence via one physical link.
Because the load balancing mode of IPv6 packets are specified, the Parameters { **src-ip** | **dst-ip** | **l4-srcport** | **l4-dstport** | **all** } of the same data stream share the same hash values after the hash algorithm, so they can be forwarded via one member interface.
Run the no command. If all the configurations of IPv6 field are deleted, the default configuration is used.

Example

Set the load balancing mode of IPv6 packets in the enhanced load balancing template 1 to dst-ip.

```
switch(config-schedule-profile-1)#ipv6 field dst-ip
switch(config-schedule-profile-1)#
```

2.6.9 l2 field

Function

The **l2 field** command configures the load balancing mode of L2 packets in the enhanced load balancing template.
The **no l2 field** command deletes the configured load balancing mode of L2 packets in the enhanced load balancing template.

Format

- **l2 field** { **src-mac** | **dst-mac** | **all** | **default** }
- **no l2 field** { **src-mac** | **dst-mac** }

Parameters

Parameters	Description	Value
src-mac	Specifies load balancing based on the source	-

Parameters	Description	Value
	MAC address.	
dst-mac	Specifies load balancing based on the destination MAC address.	-
default	Restores default settings.	-
all	Specifies load balancing based on all of the preceding fields.	-

Default Value

By default, the load balance mode of L2 packets is set to src-mac and dst-mac.

View

Schedule-profile configuration view

Usage Guidelines

If this command is executed for multiple times, the load balancing mode configured for L2 packets by the last command applies.
If you run the no l2 field command to delete all configuration of the L2 field, the configuration restores to the default configuration.

Example

Set the load balancing mode of L2 packets in the enhanced load balancing template 123 to all.

```
switch(config-schedule-profile-1)#l2 field all
switch(config-schedule-profile-1)#
```

2.6.10 mode

Function

The **mode** command sets or changes the working mode of a trunk interface.

Format

- **mode** { **manual** | **lacp-static** }

Parameters

Parameters	Description	Value
manual	Sets the working mode to manual load balancing.	-
lacp-static	Sets the working mode to static LACP.	-

Default Value

By default, a trunk interface works in manual load balancing mode.

View

Interface configuration view (trunk)

Usage Guidelines

The switch supports two trunk interface working modes:

- Manual load balancing mode: You need to manually create a trunk interface and add member interfaces to it. Multiple member interfaces manually added to the trunk interface can perform load balancing.
- Static LACP mode: The two ends of the link use the LACP protocol to negotiate trunk interface Parameters and choose active member interfaces to forward data traffic.

Before changing the working mode of a trunk interface, make sure that the trunk interface does not contain any member interfaces.

Example

Create trunk 1 and configure it to work in static LACP mode.

```
switch(config-eth-trunk-1)#mode lacp-static
switch(config-eth-trunk-1)#
```

2.6.11schedule-profile

Function

The **schedule-profile** command creates an enhanced load balancing template and enters the template view.
The **no schedule-profile** command deletes the enhanced load balancing template.

Format

- **schedule-profile** *profile-name*
- **no schedule-profile** *profile-name*

Parameters

Parameters	Description	Value
profile-name	Specifies the name of the enhanced load balancing template.	The value is a string of 1 to 33 characters.

Default Value

None

View

Global configuration view

Usage Guidelines

Currently, the switch supports only one enhanced load balancing template.

Example

Create an enhanced load balancing template named 1 and enter the template view.

```
switch(config)#schedule-profile 1
switch(config-schedule-profile-1)#
```

2.6.12 show interface eth-trunk verbose

Function

The **show interface eth-trunk** command displays the configuration of a trunk interface.

Format

- **show interface eth-trunk** *trunk-number* **verbose**
- **show interface eth-trunk verbose**

Parameters

Parameters	Description	Value
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.

Default Value

None

View

Privileged user view, global configuration view, common user view, schedule-profile configuration view

Usage Guidelines

You can use this command to check the list of physical interfaces bound to a trunk interface and load balancing mode of the trunk interface.

Example

Display the configuration of trunk 1.

```
switch#show interface eth-trunk verbose
 Unknown-unicast-Alg:srcdst-mac

 Interface eth-trunk1:
  Schedule-Alg:src-mac
  Interface Mode:lacp
  Port-List:
   Interface                 State(a/o)      InUtil              OutUtil
   100gigaethernet1/0/8      up/up             0.00%               0.00%
   100gigaethernet1/0/7      up/up             0.00%               0.00%
```

```
  100gigaethernet1/0/6      up/down          0.00%              0.00%
  100gigaethernet1/0/5      up/up            0.00%              0.00%
  100gigaethernet1/0/4      up/up            0.00%              0.00%
 Max-BW:(M):500000
 Cur-BW:(M):0

switch#
```

2.6.13 show lacp config

Function

The **show lacp config** command displays the LACP configuration on the switch.

Format

- **show lacp config**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (trunk and Ethernet trunk member)

Usage Guidelines

None

Example

Display LACP system information.

```
switch#show lacp config
Version : LACP_VB3.00.00.00
interface eth-trunk-2
  mode lacp-static
switch#
```

2.6.14 show lacp eth-trunk

Function

The **show lacp eth-trunk** command displays information about an LACP trunk interface.

Format

- **show lacp eth-trunk**
- **show lacp eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (trunk and Ethernet trunk member)

Usage Guidelines

None

Example

Display information about an LACP trunk interface.

```
switch#show lacp eth-trunk
  Interface          Status      PortNum     MainPort      MaxActiveIfNum
  eth-trunk-1        master      0           ------        8
switch#show lacp eth-trunk 1
eth-trunk-1:
  LACP Status: master
  System Priority: 1
  System Mac Address: 00:00:02:90:ff:ff
  Number Of Port In Trunk: 0
  Max Active port number: 8
switch#
```

2.6.15 show lacp statistic interface eth-trunk

Function

The **show lacp statistic interface eth-trunk** command displays the Tx and Rx LACP packet statistics in LACP mode.

Format

- **show lacp statistic interface eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (trunk and Ethernet trunk member)

Usage Guidelines

This command requires the aggregation mode to be LACP. To modify the working mode to LACP, run the modecommand in the Eth-Trunk interface view.
To view the statistics of a specified aggregation group, the aggregation group must be existing. To view the statistics of a specified interface of a specified aggregation group, run the addcommand to add the interface into the group.

Example

View the Tx and Rx LACP packet statistics in LACP mode.

```
switch#show lacp statistic interface eth-trunk 1
  Interface eth-trunk-1 PDU statistic info :
  Port              LacpRevPdu      LacpSentPdu     MarkerRevPdu    MarkerSentPdu
  10ge-1/0/1          0               0               0               0
switch#
```

2.6.16 show lacp system

Function

The **show lacp system** command displays LACP system information.

Format

- **show lacp system**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (trunk and Ethernet trunk member)

Usage Guidelines

None

Example

Display LACP system information.

```
switch#show lacp system
LACP system information:
        Max AG number: 128
        System Priority: 32768
        System Mac Address: 00:00:02:90:ff:ff
        Fast Periodic Time: 1(s)
        Slow Periodic Time: 30(s)
        Short Timeout Time: 3(s)
        Long Timeout Time: 90(s)
        Churn Detection Time: 60(s)
        Join Ag waiting time: 2(s)
```

2.6.17 show schedule-profile

Function

The **show schedule-profile** command shows details of the enhanced load balancing template.

Format

- **show schedule-profile**
- **show schedule-profile** *name*

Parameters

Parameters	Description	Value
name	Specifies the name of the enhanced load balancing template.	The value is a string of 1 to 33 characters.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Trunk), Schedule-profile configuration view

Usage Guidelines

You can use this command to view details about the enhanced load balancing template, including the load balancing settings of L3 IPv4 packets and L2 packets.

Example

Show details of enhanced load balancing template test.

```
switch#show schedule-profile test
 Version : SCHEDULEPROFILE_VB3.00.00.00
 schedule-profile: test
  Packet      HashField
  L2          src-mac      dst-mac
  IPV4        src-ip       dst-ip
  MPLS        top-label    2nd-label
```

2.7 Mlag Configuration Commands

2.7.1 debug mlag

Function

The **debug mlag** command enables MLAG debugging.
The **no debug mlag** command disables **mlag** debugging.

Format

- **debug mlag { in | out | timer | notify | global | if | packet | error | all }**
- **no debug mlag { in | out | timer | notify | global | if | packet | error | all }**

Parameters

Parameters	Description	Value
In	Receive packet information	-
out	Sending packet information	-
timer	Timer information	-
notify	Notify information	-
global	global information	-
if	interface information	-
error	Error information	-
default	All information	-
all	Receive packet information	-

Default Value

disable

View

Privileged user view

Usage Guidelines

None

Example

Enable MLAG debugging.

```
switch#debug mlag all
switch#
```

2.7.2 lacp mlag priority

Function

The **lacp mlag priority** command sets the LACP **mlag** priority.

Format

lacp mlag priority { *priority-value* | **default** }

Parameters

Parameters	Description	Value
priority-value	Specify the system priority of LACP MLAG, the smaller the value, the higher the LACP priority	The value is an integer in the range from1 to 65535
default	Uses the default LACP MLAG priority value.	32768

Default Value

None

View

Global configuration view

Usage Guidelines

The system priority of LACP MLAG configured in the global configuration view is valid for all Eth-Trunk interfaces.
When an M-LAG is composed of an Eth-Trunk in LACP mode, the LACP M-LAG system priority is used to differentiate priorities of the devices at both sides of the Eth-Trunk. The device with a higher system priority functions as the Actor, and the other device selects the active interface based on the interface priority of the Actor.

Example

Set the LACP MLAG system priority

```
switch(config)#lacp mlag priority 10
switch(config)#
```

2.7.3 lacp mlag system-id

Function

The lacp mlag system-id command displays LACP MLAG system-id.

Format

lacp mlag system-id *mac-address*

Parameters

Parameters	Description	Value
mac-address	Specify the system ID of LACP MLAG, the smaller the system ID value, the higher the priority	The value is in the AA:BB:CC:DD:EE:FF format, where each of the letters A to F represents a hexadecimal digit.

Default Value

Deafult value is the switch of MAC-address.

View

Global configuration view

Usage Guidelines

The LACP MLAG system ID configured in the global configuration view is valid for all Eth-Trunk interfaces.
When both ends of the Eth-Trunk use the same LACP M-LAG system priority, you can run the **lacp m-lag system-id** command to set the LACP M-LAG system ID to determine priorities of the two devices. The devices then can determine active interfaces.

Example

Display LACP MLAG system-id.

```
switch(config)#lacp mlag system-id 04:f8:f8:e5:b8:ba
switch(config)#
```

2.7.4 mlag exclude interface

Function

mlag exclude interfae command is used to configure the exclude interface of cross-device link aggregation.

no mlag exclude interface command is used to delete the exclude interface of cross-device link aggregation.

Format

- **mlag exclude interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **mlag exclude interface bridge-domain domain-number**
- **mlag exclude interface eth-trunk trunk-number**
- **mlag exclude interface loopback loopback-number**
- **mlag exclude interface vlan vlan-id**
- **no mlag exclude interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } interface-number**
- **no mlag exclude interface bridge-domain domain-number**
- **no mlag exclude interface eth-trunk trunk-number**
- **no mlag exclude interface loopback loopback-number**
- **no mlag exclude interface vlan vlan-id**

Parameters

Parameters	Description	Value
interface-number	Specify the Ethernet port number	The value is an integer in the range of<1-1>/<0-1>/<1-48>
domain-number	Specify the bridge-domain number ID	The value is an integer in the range from 1 to 1048576
trunk-number	Specify the Trunk interface number	The value is an integer in the range from 1 to 128
loopback-number	Specify the loopback number ID	The value is an integer in the range from 1 to 127
vlan-id	Specify the VLAN ID	The value is an integer in the range from 1 to 4094

Default Value

None

View

global configuration view

Usage Guidelines

None

Example

Configure the exclude interface

```
switch(config)#mlag exclude interface xgigaethernet 1/0/1
switch(config)#
```

2.7.5 mlag-group

Function

The **mlag-group** command adds an interface to a mlag-group.
The **no join mlag** command deletes an interface from a mlag-group.

Format

- **mlag-group mlag-group**
- **no mlag-group mlag-group**

Parameters

Parameters	Description	Value
mlag-group	Specify the MLAG group index number	The value is an integer in the range of <1-1>

Default Value

None

View

global configuration view

Usage Guidelines

None

Example

Add interface to a mlag-group.

```
switch(config)#mlag-group 1
switch(config-mlag-1)#
```

2.7.6 mlag interface eth-trunk

Function

The **mlag interface eth-trunk** command creates a trunk interface and displays the trunk interface configuration view.
The **no mlag** command deletes an existing mlag-member interface configuration view.

Format

- **mlag mlag-member interface eth-trunk trunk-number**
- **no mlag mlag-member**

Parameters

Parameters	Description	Value
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 128.
mlag-member	Specifies a MLAG-member interface ID.	The value is an integer in the range from 1 to 128.

Default Value

None

View

MLAG configuration view

Usage Guidelines

None

Example

Enter the configuration view of MLAG interface 1, configure aggregation group Eth-trunk 1 as MLAG member.

```
switch(config-mlag-1)#mlag 1 interface eth-trunk 1
switch(config-mlag-1)#
```

2.7.7 peerlink exclude

Function

peerlink exclude command specifies VLANs not allowed by a peer-link interface.
no peerlink exclude command cancels the configuration.

Format

- **peerlink exclude vlan-list**
- **no peerlink exclude vlan-list**

Parameters

Parameters	Description	Value
vlan-list	Specifies VLANs not allowed by a peer-link interface	The value is an integer in range from 1 to 4094

Default Value

None

View

MLAG Configuration view

Usage Guidelines

None

Example

#Specify VLANs 10 to 30 not allowed by Eth-Trunk 2

```
switch(config-mlag-1)#peerlink exlcude 2
switch(config-mlag-1)#
```

2.7.8 peerlink interface eth-trunk

Function

peerlink interface eth-trunk configures an eth-trunk interface as the peer-link interface.
no peerlink interface deletes the peer-link interface.

Format

- **peerlink interface eth-trunk trunk-number**
- **no peerlink interface**

Parameters

Parameters	Description	Value
trunk-number	Specify the Eth-trunk interface port number	The value is an integer in range from 1 to 128

Default Value

None

View

MLAG configuration view

Usage Guidelines

None

Example

#Configure the Eth-trunk interface as peer-link interface

```
switch(config-mlag-1)#peerlink interface eth-trunk 1
switchconfig-mlag-1)#
```

2.7.9 priority

Function

The **priority** command configures the MLAG priority.

Format

priority { *priority-value* | **default** }

Parameters

Parameters	Description	Value
priority-value	Specifies the MLAG priority.	The value is an integer in the range from 1 to 255.
default	Specifies the default mlag priority.	The value is 1.

Default Value

The default is 1.

View

MLAGconfiguration view

Usage Guidelines

Two devices configured with M-LAG send negotiation packets for negotiation and determine the master and backup statuses. M-LAG determines the master and backup statuses based on the priority and MAC address. The device with a higher priority is the master. You can also run the priority command to set the priority to determine the master and backup statuses of devices.

Example

Set MLAG priority .

```
switch(config-mlag-1)#priority 10
switch(config-mlag-1)#
```

2.7.10 reset counter

Function

The **reset counter** command resets the count of MLAG.

Format

reset counter

Parameters

None

Default Value

None

View

MLAG configuration view

Usage Guidelines

None

Example

resets the count of MLAG.

```
switch(config-mlag-1)#reset counter
switch(config-mlag-1)#
```

2.7.11security-key

Function

security-key command is used to configure security key.
no security-key command is used to delete the configuration of security key.

Format

- **security-key { simple | md5 } { plain | cipher }key**
- **no security-key**

Parameters

Parameters	Description	Value
simple	Specify a simple password	-
md5	Specify a MD5 text password	-
plain	Specify a plain password	-
cipher	Specify a cipher password	-
key	Specify the Secure password string	The value is a string up to 15 characters

Default Value

None

View

MLAG configuration view

Usage Guidelines

None

Example

#Configure security-key password

```
switch(config-mlag-1)#security-key simple abcdefg
switch(config-mlag-1)#
```

2.7.12 show mlag

Function

The **show mlag** command displays MLAG information .

Format

- **show mlag**

Parameters

None

Default Value

None

View

Common user view

Usage Guidelines

None

Example

Show all MLAG information.

```
switch#show mlag
Max mlag group number      :1
Current mlag group number:1
lacp system-id             :68:21:5f:dc:25:02
lacp priority              :32768
The MLAG group 1 information:
  Priority                 :10
  Peerlink                 :eth-trunk 128
  Role                     :BACKUP          PeerRole              :MASTER
  Send-Period (1s)         :3               Fail-Time (1s)        :9
  ProtoType                :layer2          Peer-Priority         :1
  Peer-Send-Time           :3               Peer-Fail-Time        :9
  Security-Key-Type        :md5             Security-Key          :fs
  Source-IP                :2000:100::2     Peer-IP               :2000:100::1
```

```
DAD detect state        :OK                 DAD conflict state      :NORMAL
  In                     :5797               Out                     :5797
  InDrop                 :0                  OutDrop                 :2
  In DAD                 :10433              Out DAD                 :17346
  In DAD error           :0                  Out DAD fail            :3
switch#
```

2.7.13 show mlag config

Function

The **show mlag config** command displays the MLAG configuration.

Format

- **show mlag config**

Parameters

None

Default Value

None

View

Common user view

Usage Guidelines

None

Example

Display MLAG system information.

```
switch# show mlag config
!
lacp mlag system-id 68:21:5f:dc:25:02
mlag-group 1
 peerlink interface eth-trunk 128
 priority 10
 source-address 2000:100::2 vpn-instance mlag
 security-key md5 plain fs
 mlag 1 interface eth-trunk 1
switch#
```

2.7.14 show mlag consistency

Function

show mlag consistency command is used to show M-LAG information of configuration consistency

Format

- **show mlag consistency**

Parameters

None

Default Value

None

View

Common user view

Usage Guidelines

None

Example

Show M-LAG information of configuration consistency.

```
switch#show mlag consistency
------------------------------------------------------------
Configuration           Local value                 Peer value
------------------------------------------------------------
------------------------ STP -------------------------------
--------------------------- VLAN -----------------------------

VLAN:3858
VLANIF(STATUS)          up                            N/A
VLANIF(VRRP)            ipv6 vrrpv3                 N/A

VLAN:3859
VLANIF(STATUS)          up                            N/A
VLANIF(VRRP)            ipv6 vrrpv3                 N/A

VLAN:3860
VLANIF(STATUS)          up                            N/A
VLANIF(VRRP)            ipv6 vrrpv3                 N/A

VLAN:3861
```

```
VLANIF(STATUS)          up                          N/A
VLANIF(VRRP)            ipv6 vrrpv3                 N/A
……
switch#
```

2.7.15 show mlag exclude interface

Function

show mlag exclude interface command is used to display m-lag exclude interface.

Format

- **show mlag exclude interface**

Parameters

None

Default Value

None

View

Common user view

Usage Guidelines

None

Example

Display m-lag exclude interface

```
switch(config)#interface vlan 3
switch#show mlag exclude interface
  Mlag Default Exclude Interface
                        25ge1/0/5
                       25ge1/0/48
                       100ge1/1/2
switch#
```

2.7.16 show mlag-group

Function

show mlag-group command is used to display m-lag group information.

Format

- **show mlag-group mlag-group**

Parameters

Parameters	Description	Value
mlag-group	Display the MLAG group index number	The value is an integer in range from <1-1>

Default Value

None

View

Common user view

Usage Guidelines

None

Example

Display m-lag group information

```
switch#show mlag-group 1
The MLAG group 1 information:
  Priority                :10
  Peerlink                :eth-trunk 128
  Role                    :BACKUP          PeerRole              :MASTER
  Send-Period (1s)        :3               Fail-Time (1s)        :9
  ProtoType               :layer2          Peer-Priority         :1
  Peer-Send-Time          :3               Peer-Fail-Time        :9
  Security-Key-Type       :md5             Security-Key          :fs
  Source-IP               :2000:100::2     Peer-IP               :2000:100::1
  DAD detect state        :OK              DAD conflict state    :NORMAL
  In                      :5852            Out                   :5853
  InDrop                  :0               OutDrop               :2
  In DAD                  :10534           Out DAD               :17513
  In DAD error            :0               Out DAD fail          :3
                  The Member information(Total number 1)
  MLAG ID     Trunk ID      State(a/o)     PeerValid     Peer ID      PeerState
  1           1             down/down      VALID         1            up

switch#
```

2.7.17 source-address

Function

source-address command is used to configure the local source IPv4 /IPv6 address of dual-active detection.
no source-address command cancels configurations.

Format

- **source-address ipv4-address [vpn-instance name]**
- **source-address ipv6-address [vpn-instance name]**
- **no source-address**

Parameters

Parameters	Description	Value
ipv4-address	Specifies the destination IPv4 address.	The value is in dotted decimal notation.
Ipv6-address	Specifies the destination IPv6 address.	The value is of 128 digits and divided into eight groups. Each group is a hexadecimal string of four characters. The value is in X:X:X:X:X:X:X:X format.
name	VPN instance	The value is a string no more than 64 characters

Default Value.

None

View

MLAG configuration view

Usage Guidelines

None

Example

#Configure local source IPv4/IPv6 address of dual-active detection

```
switch(config-mlag-1)#source-address 10.18.12.11
switch(config-mlag-1)#
```

2.7.18 stp v-stp enable

Function

stp v-stp enable command enables v-stp on M-LAG device.

Format

- **stp v-stp {enable | disable }**

Parameters

None

Default Value

By default, v-stp is disabled.

View

stp configuration view

Usage Guidelines

None

Example

Enable v-stp on an M-LAG device.

```
switch(config-stp)#stp v-stp enable
```

2.7.19 timer hello

Function

timer hello command is used to configure hello packet timer.

Format

- **timer hello { hello-interval | default }**

Parameters

Parameters	Description	Value
hello-interval	Specify hello packet interval	The value is an integer in range from 3 to 30
default	Specify the default hello packet interval	3 second

Default Value

3 second

View

MLAG configuration view

Usage Guidelines

None

Example

Configure Hello packet interval

```
switch(config-mlag-1)#timer hello 10
switch(config-mlag-1)#
```

2.7.20 timer hold-on-failure multiplier

Function

timer hold-on-failure multiplier command is used to configure a timer that is a multiple of hello packet interval.

Format

- **timer hold-on-failure multiplier { value | default }**

Parameters

Parameters	Description	Value
value	Specify the timer that is a multiple of hello packet interval	The value is an integer in range from 3 to 15
default	The default value of timer	3

Default Value

Three

View

MLAG configuration view

Usage Guidelines

None

Example

#Configure a timer that is a multiple of the hello interval.

```
switch(config-mlag-1)#timer hold-on-failure multiplier 5
switch(config-mlag-1)#
```

2.7.21 up-delay

Function

up-delay command is used to set a delay for the M-LAG member interface to report the up event.

Format

- **up-delay { delay-value | default } [auto-recovery interval { interval-value | default }]**

Parameters

Parameters	Description	Value
delay-value	Specify the delay value for the M-LAG member interface to report the up event.	The value is an integer that ranges from 0 to 3600, in seconds.
default	Specify the default delay value for the M-LAG member interface to report the up event.	240 seconds

Parameters	Description	Value
interval-value	Specify the automatic recovery interval between M-LAG member interfaces based on the delay in reporting the up event.	The value is an integer that ranges from 0 to 180, in seconds
default	Specify the default automatic recovery interval.	0

Default Value

Delay-value: 240s

View

MLAG configuration view

Usage Guidelines

None

Example

#Configure a delay for the M-LAG member interface to report the Up event as 90s.

```
switch(config-mlag-1)#up-delay 90
switch(config-mlag-1)#
```

2.8 VLAN Configuration Commands

2.8.1 interface vlan

Function

The **interface vlan** command enables the system to display the VLANIF interface configuration view.
The **no interface vlan** command deletes a VLANIF interface.

Format

- **interface vlan** *vlan-id*
- **no interface vlan** *vlan-id*

Parameters

Parameters	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Enter the view of VLAN interface 3.

```
switch(config)#interface vlan 3
switch(config-vlanif-3)#
```

2.8.2 port default vlan

Function

The **port default vlan** command specifies the default VLAN of an interface and adds the interface to the VLAN.
The **no port default vlan** command deletes the default VLAN of an interface and exits the VLAN.

Format

- **port default vlan** *vlan-id*
- **no port default vlan**

Parameters

Parameters	Description	Value
vlan-id	Specifies the default VLAN ID of an interface.	The value is an integer in the range from 1 to 4094.

Default Value

The default VLAN is VLAN 1 and interfaces are added to VLAN 1 in untagged mode by default.

View

Interface configuration view (10GE / 100GE / Trunk) and interface group configuration view

Usage Guidelines

This command is valid only to interfaces in the Access and QinQ types. The VLAN specified by *vlan-id* must exist.
The switch interface can belong to multiple VLANs. If a default VLAN is configured, the interface handles the packets in the following ways:

- Upon receiving packets without VLAN tags, the interface adds VLAN tags to the packets and sets the VID in the tag to the default VLAN ID of the interface.
- When the interface receives a VLAN tagged packet carrying the same VLAN ID as the default VLAN ID of the interface, the packet is forwarded though the interface. If the VLAN ID of the packet is different from the default VLAN ID of the interface, the packet is dropped.

- When the interface receives a VLAN tagged packet carrying the same VLAN ID as the default VLAN ID of the interface, the interface removes the VLAN tag from the packet and then sends the packet.

Example

Set the default VLAN of interface 10gigaethernet1/0/1 to VLAN 2.

```
switch(config-10ge1/0/1)#port link-type access
switch(config-10ge1/0/1)#port default vlan 2
switch(config-10ge1/0/1)#
```

2.8.3 port hybrid vlan

Function

The **port hybrid vlan** command specifies one or more VLANs to which a hybrid interface belongs.
The **no port hybrid vlan** command deletes one or more VLANs to which a hybrid interface belongs.

Format

- **port hybrid vlan** *vlan-list* { **tagged** | **untagged** }
- **no port hybrid vlan** *vlan-list*
- **no port hybrid vlan all**

Parameters

Parameters	Description	Value
vlan-list	*Mandatory.* Specifies the VLAN ID of a hybrid interface.	The value is an integer in the range from 1 to 4094.
tagged	Indicates that VLAN frames pass through the interface with tags.	-
untagged	Indicates that VLAN frames pass through the interface without tags.	-

Default Value

None

View

Interface configuration view (10GE / 100GE / Trunk) and interface group configuration view

Usage Guidelines

You can use this command to add hybrid interfaces to the VLAN in tagged or untagged mode. Where:
Tagged: Indicates that the interface does not remove the VLAN tag from a frame when sending the frame.
Untagged: Indicates that the interface removes the VLAN tag from a frame when sending the frame.
You can add a hybrid interface to multiple VLANs at a time.

Example

Configure interface to remove VLAN tags when sending VLAN2 frames.

```
switch(config-10ge1/0/1)#port hybrid vlan 2 untagged
switch(config-10ge1/0/1)#
```

2.8.4 port hybrid pvid

Function

The **port hybrid pvid** command specifies the default VLAN of a hybrid interface.

Format

- **port hybrid pvid** { *vlan-id* | **default** }

Parameters

Parameters	Description	Value
vlan-id	Configures the Default Value VLAN ID of the hybrid interface.	The value is an integer in the range from 1 to 4094.
default	Configures the Default Value VLAN ID of the hybrid interface.	The Default Value is VLAN1.

Default Value

The default VLAN ID of the hybrid interface is VLAN1.

View

Interface configuration view (10GE / 100GE / Trunk) and interface group configuration view

Usage Guidelines

After the default VLAN ID is configured for a hybrid interface, you must add the interface to the default VLAN so that the interface can send packets with the default VLAN tag.
For details of adding a hybrid interface to the VLAN, see **port hybrid vlan**.

Example

Set the default VLAN of hybrid interface 10gigaethernet1/0/1 to VLAN 25.

```
switch(config-10ge1/0/1)#port hybrid pvid 25
switch(config-10ge1/0/1)#
```

2.8.5 port link-type

Function

The **port link-type** command sets the link type (interface type) of an interface.

Format

- **port link-type** { **access** | **trunk** | **hybrid** | **default** }

Parameters

Parameters	Description	Value
access	Sets the interface type to Access.	-
trunk	Sets the interface type to Trunk.	-
hybrid	Sets the interface type to Hybrid.	-
default	Restores the interface type to the default, that is, Hybrid.	-

Default Value

Hybrid

View

Interface configuration view (10GE / 100GE / Trunk) and interface group configuration view

Usage Guidelines

- Access interface: Generally, it is connected to the host. It can only connect to the access link and transmit Ethernet frames without VLAN tags. If the access interface is configured with a default VLAN, packets are added with the default VLAN tag. The link allows Ethernet frames matching the default VLAN tag to pass through.
- Trunk interface: Generally, it is connected to network devices such as the switch or router. It can connect to only the trunk link. It allows multiple VLAN frames to pass through the link.
- Hybrid interface: It can be connected to both a host (access link) and a network device (trunk link). It allows multiple VLAN frames to pass through and removes tags of certain VLAN frames in the outbound direction.

Note: Before changing the interface type, delete the original VLAN configuration. That is, restore the setting of the interface to the default configuration (being added to only VLAN1).

Example

Set the interface type to Access.

```
switch(config-10ge1/0/1)#port link-type access
switch(config-10ge1/0/1)#
```

2.8.6 port trunk allow-pass vlan

Function

The **port trunk allow-pass vlan** command adds a trunk interface to specified VLANs.
The **no port trunk allow-pass vlan** command removes a trunk interface from specified VLANs.

Format

- **port trunk allow-pass vlan** *vlan-list*

- **port trunk allow-pass vlan all**
- **no port trunk allow-pass vlan** *vlan-list*
- **no port trunk allow-pass vlan all**

Parameters

Parameters	Description	Value
vlan-list	Specifies the list of VLANs to which the trunk interface belongs.	The value is an integer in the range from 1 to 4094, for example, 1, 3, 5, and 8.

Default Value

None

View

Interface configuration view (10GE / 100GE / Trunk) and interface group configuration view

Usage Guidelines

You can use this command to add the trunk interface to the VLAN in a tagged mode. In this way, the interface does not remove the VLAN tags from frames it sends.
The VLAN specified in the VLAN list must exist. Otherwise, the configuration is invalid.
You cannot use this command for physical interfaces added to the aggregation interface.

Example

Add the trunk interface 10gigaethernet 1/0/1 into VLAN 2.

```
switch(config-10ge1/0/1)#port link-type trunk
switch(config-10ge1/0/1)#port trunk allow-pass vlan 2
switch(config-10ge1/0/1)#
```

2.8.7 port trunk pvid

Function

The **port trunk pvid** command specifies the default VLAN of a trunk interface.

Format

- **port trunk pvid** { *vlan-id* | **default** }

Parameters

Parameters	Description	Value
vlan-id	Configures the Default Value VLAN ID of the trunk interface.	The value is an integer in the range from 1 to 4094.
default	Restores the VLAN ID of the trunk interface to the Default Value.	The Default Value is VLAN1.

Default Value

The default VLAN ID of the trunk interface is VLAN1.

View

Interface configuration view (10GE / 100GE / Trunk) and interface group configuration view

Usage Guidelines

After the default VLAN ID is configured for a trunk interface, you must add the interface to the default VLAN so that the interface can send packets with the default VLAN tag.
For details of adding a trunk interface to the VLAN, see port trunk pvid.

Example

Set the default VLAN of trunk interface 10gigaethernet1/0/1 to VLAN 2.

```
switch(config-10ge1/0/1)#port link-type trunk
switch(config-10ge1/0/1)#port trunk pvid 2
switch(config-10ge1/0/1)#
```

2.8.8 show interface vlan config

Function

The **show interface vlan config** command displays the VLAN interface configuration.

Format

- **show interface vlan** *vlan-id* **config**
- **show interface vlan config**

Parameters

Parameters	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

Common user view, privileged user view, global configuration view, and VLANIF configuration view

Usage Guidelines

None

Example

Show the configuration of the VLAN interface.

```
switch#show interface vlan 1 config
switch#
```

2.8.9 show vlan

Function

The **show vlan** command displays VLAN information on the switch.

Format

- **show vlan**
- **show vlan all**
- **show vlan all** *vlan-list*
- **show vlan** *vlan-id*
- **show vlan property** *vlan-list*
- **show vlan verbose**

Parameters

Parameters	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer in the range from 1 to 4094.
vlan-list	Specifies the VLAN list.	The value is an integer string, in the format like 1, 2, and 3-5.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (10GE / 100GE / Trunk), VLANIF configuration view, VLAN configuration view, interface group configuration view

Usage Guidelines

The **show vlan** command shows all VLAN configuration, including the VLAN ID, type, state, and MAC address learning state.
The **show vlan verbose** command shows all VLAN details.
The **show vlan** *vlan-id* **verbose** command shows details of a specific VLAN, including the VLAN ID, type, description, state, measurement state, interface, and interface joining mode.

Example

Show all VLAN-related information.

```
switch#show vlan
  Total :3      Static :3      Dynamic :0
  -=None, M=Member,U=Untagged
  VID     100ge1/0/1-10ge1/0/34
  1       UUUU UUUU UUUU UUUU UUUU UUUU UUUU UUUU UU
```

```
  VID    100ge1/0/1-10ge1/0/34
  2      -M-- ---- ---- ---- ---- ---- ---- --
  VID    100ge1/0/1-10ge1/0/34
  3      -M-- ---- ---- ---- ---- ---- ---- --
switch#
```

2.8.10 show port vlan

Function

The **show port vlan** command displays the interfaces in a VLAN.

Format

- **show port vlan**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (10GE / 100GE / Trunk), VLANIF configuration view, VLAN configuration view, interface group configuration view

Usage Guidelines

None

Example

View the interfaces in a VLAN.

```
switch#show port vlan
Interface                Link Type    PVID    VLAN List
mgt-eth 0/0/0             hybrid       0
100gigaethernet 1/0/1    hybrid       1       1
100gigaethernet 1/0/2    trunk        1       1-3
100gigaethernet 1/0/3    hybrid       1       1
100gigaethernet 1/0/4    hybrid       1       1
100gigaethernet 1/0/5    hybrid       1       1
100gigaethernet 1/0/6    hybrid       1       1
100gigaethernet 1/0/7    hybrid       1       1
100gigaethernet 1/0/8    hybrid       1       1
100gigaethernet 1/0/9    hybrid       1       1
100gigaethernet 1/0/10   hybrid       1       1
```

100gigaethernet 1/0/11	hybrid	1	1
100gigaethernet 1/0/12	hybrid	1	1
100gigaethernet 1/0/13	hybrid	1	1
100gigaethernet 1/0/14	hybrid	1	1
100gigaethernet 1/0/15	hybrid	1	1
100gigaethernet 1/0/16	hybrid	1	1
100gigaethernet 1/0/17	hybrid	1	1
100gigaethernet 1/0/18	hybrid	1	1
100gigaethernet 1/0/19	hybrid	1	1
100gigaethernet 1/0/20	hybrid	1	1
100gigaethernet 1/0/21	hybrid	1	1
100gigaethernet 1/0/22	hybrid	1	1
100gigaethernet 1/0/23	hybrid	1	1
100gigaethernet 1/0/24	hybrid	1	1
100gigaethernet 1/0/25	hybrid	1	1
100gigaethernet 1/0/26	hybrid	1	1
100gigaethernet 1/0/27	hybrid	1	1
100gigaethernet 1/0/28	hybrid	1	1
100gigaethernet 1/0/29	hybrid	1	1
100gigaethernet 1/0/30	hybrid	1	1
100gigaethernet 1/0/31	hybrid	1	1
100gigaethernet 1/0/32	hybrid	1	1
10gigaethernet 1/0/33	hybrid	1	1
10gigaethernet 1/0/34	hybrid	1	1
eth-trunk 1	hybrid	1	1

2.8.11tpid

Function

The **tpid** command sets the protocol ID in the outer tag of packets on the current interface.

Format

- **tpid** { ***standard*** | *protocol-id* }

Parameters

Parameters	Description	Value
protocol-id	Indicates the protocol identifier of the outer tag of the current interface.	The value is a hexadecimal number in the range from 0x600 to 0xffff.
standard	Specifies a standard value.	802.1q in 802.1q mode

Default Value

The default is 802.1q in 802.1q mode.

View

Interface configuration view (10GE / 100GE / Trunk) and interface group configuration view

Usage Guidelines

Because different vendors use different protocols for outer tags to achieve the QinQ function, you must run the **tpid** command to configure the protocol identifier of the outer tag of the current interface when the switch interconnects a device provided by another vendor.

Example

Set the TPID of the outer tag of interface 10gigaethernet1/0/1 to 0x8000.

```
switch(config-10ge1/0/1)#tpid 0x8000
switch(config-10ge1/0/1)#
```

2.8.12 unknown-multicast {forward|drop}

Function

The **unknown-multicast {forward|drop}** command configures the processing of unknown multicast packets during the VLAN packet forwarding.

Format

- **unknown-multicast** { **forward** | **drop** }

Parameters

Parameters	Description	Value
forward	Forwards unknown multicast packets.	-
drop	Drops unknown multicast packets.	-

Default Value

The default is forward.

View

VLAN configuration view

Usage Guidelines

None

Example

Configure VLAN2 node to directly discard unknown multicast packets.

```
switch(vlan-2)#unknown-multicast drop
switch(vlan-2)#
```

2.8.13 vlan unknown-multicast {forward|drop}

Function

The **vlan unknown-multicast {forward|drop}** command configures the processing of unknown multicast packets during the VLAN packet forwarding.

Format

- **vlan** *vlan-id* **unknown-multicast** { **forward** | **drop** }
- **unknown-multicast vlan** *vlan-list* { **forward** | **drop** }

Parameters

Parameters	Description	Value
forward	Forwards unknown multicast packets.	-
drop	Drops unknown multicast packets.	-
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.

Default Value

The default is forward.

View

Global configuration view

Usage Guidelines

None

Example

Globally configure the VLAN10 to discard unknown multicast packets.

```
switch(config)#vlan 10 unknown-multicast drop
switch(config)#
```

2.8.14 unknown-unicast {forward|drop}

Function

The **unknown-unicast {forward|drop}** command configures the processing of unknown unicast packets during the VLAN packet forwarding.

Format

- **unknown-unicast** { **forward** | **drop** }

Parameters

Parameters	Description	Value
forward	Forwards unknown multicast packets.	-
drop	Drops unknown multicast packets.	-

Default Value

The default is forward.

View

VLAN configuration view

Usage Guidelines

None

Example

Configure VLAN2 node to directly discard unknown unicast packets.

```
switch(vlan-2)#unknown-multicast drop
switch(vlan-2)#
```

2.8.15 vlan unknown-unicast {forwad|drop}

Function

The **vlan unknown-unicast {forwad|drop}** command configures the processing of unknown unicast packets during the VLAN packet forwarding.

Format

- **vlan** *vlan-id* **unknown-unicast** { **forward** | **drop** }
- **unknown-multicast vlan** *vlan-list* { **forward** | **drop** }

Parameters

Parameters	Description	Value

Parameters	Description	Value
forward	Forwards unknown multicast packets.	-
drop	Drops unknown multicast packets.	-
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.

Default Value

The default is forward.

View

Global configuration view

Usage Guidelines

None

Example

Globally configure the VLAN2 to discard unknown unicast packets.

```
switch(config)#vlan 2 unknown-unicast drop
switch(config)#
```

2.8.16 vlan-trunk {enable|disable}

Function

The **vlan-trunk {enable|disable}** command enables or disables automatic VLAN creation.

Format

- **vlan-trunk** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables automatic VLAN creation.	-
disable	Disables automatic VLAN creation.	-

Default Value

disable

View

Global configuration view

Usage Guidelines

This command can create all the VLANs.

Example

Enable automatic VLAN creation.

```
switch(config)#vlan-trunk enable
switch(config)#
```

2.8.17 vlan

Function

The **vlan** command creates a VLAN and enters the VLAN view.
The **no vlan** command deletes a VLAN or multiple VLANs in batches.

Format

- **vlan** *vlan-id1* [*vlan-id2]*
- ***vlan*** *vlan-list*
- **no vlan** *vlan-id1* [*vlan-id2]*
- **no** ***vlan*** *vlan-list*

Parameters

Parameters	Description	Value
vlan-list	Specifies the VLAN list.	-
vlan-id1	vlan-id1: mandatory. Specifies the start VLAN ID.	The value is an integer in the range from 1 to 4094.
vlan-id2	vlan-id2: optional. Specifies the end VLAN ID. vlan-id2 must be larger than vlan-id1 and it determines a range together with vlan-id1. If vlan-id2 is not specified, you can create or delete the VLAN specified by vlan-id1 and enter the VLAN view.	The value is an integer in the range from 1 to 4094.

Default Value

By default, VLAN 1 exists in the system and all interfaces are added to VLAN 1 by default.

View

Global configuration view

Usage Guidelines

You can use this command to create one or more VLANs. If only one Parameters is specified, the system creates a VLAN and enters the VLAN view. If two Parameters are specified, the system creates multiple VLANs in the range specified by the start VLAN ID and end VLAN ID in the two Parameters.

VLAN 1 already exists in the system. You cannot delete it.

Example

Create VLAN 2.

```
switch(config)#vlan 2
switch(vlan-2)#
```

2.8.18 no vlan

Function

The **no vlan** command deletes a specific VLAN and exits the current VLAN configuration view.

Format

- **no vlan** *vlan-id*

Parameters

Parameters	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

VLAN configuration view

Usage Guidelines

None

Example

Delete VLAN 2 from the VLAN 10 configuration view and exit the VLAN 10 configuration view.

```
switch(vlan-10)#no vlan 2
switch(config)#
```

2.8.19 switch vlan

Function

The **switch vlan** command creates a VLAN and access the corresponding VLAN configuration view.

Format

- **switch vlan** *vlan-id*

Parameters

Parameters	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

VLAN configuration view

Usage Guidelines

None

Example

Create VLAN 2 in the VLAN 10 configuration view and access the VLAN 2 configuration view.

```
switch(vlan-10)#switch vlan 2
switch(vlan-2)#
```

2.8.20 vlan normal

Function

The **vlan normal** command sets the VLAN type to common VLAN.

Format

- **vlan normal**

Parameters

None

Default Value

None

View

VLAN configuration view

Usage Guidelines

None

Example

Set the VLAN type to common VLAN.

```
switch(vlan-10)#vlan normal
switch(vlan-10)#
```

2.9 QinQ Configuration Commands

2.9.1 vlan-stacking {enable|disable}

Function

The **vlan-stacking {enable|disable}** command enables or disables the flexible QinQ.

Format

- **vlan-stacking** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables flexible QinQ.	-
disable	Disables flexible QinQ.	-

Default Value

None

View

Interface configuration view

Usage Guidelines

None

Example

Enables flexible QinQ.

```
switch(config-100ge1/0/1)#vlan-stacking enable
switch(config-100ge1/0/1)#
```

2.9.2 dot1q-tunnel {enable|disable}

Function

The **dot1q-tunnel {enable|disable}** command enables or disables an interface to add an outer VLAN tag with the PVID to packets. This function is called QinQ.

Format

- **dot1q-tunnel** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the interface to add a PVID tag to the outer layer of a packet.	-
disable	Disables the interface from adding a PVID tag to the outer layer of a packet.	-

Default Value

disable

View

Interface configuration view (10GE / 100GE / Trunk) and interface group configuration view

Usage Guidelines

You can use this command to add a PVID tag to the outer layer of a packet.

Example

Enable the interface QinQ function.

```
switch(config-10ge1/0/1)#dot1q-tunnel enable
switch(config-10ge1/0/1)#
```

2.9.3 vlan-stacking vlan stack-vlan

Function

The **vlan-stacking vlan stack-vlan** command configures the flexible QinQ function for a single VLAN or multiple VLANs.
The **vlan-stacking vlan stack-vlan Usage Guidelines-8021p** command configures the flexible QinQ function for a single VLAN or multiple VLANs based on the VLAN ID or 802.1p priority.
The **no vlan-stacking** command deletes the flexible QinQ configuration.

Format

- **vlan-stacking vlan** *vlan-id1* **stack-vlan** *vlan-id2*
- **vlan-stacking vlan** *vlan-id3* **to** *vlan-id4* **stack-vlan** *vlan-id2*
- **vlan-stacking vlan** *vlan-id1* **stack-vlan** *vlan-id2* **remark-8021p** *priority*
- **vlan-stacking vlan** *vlan-id3* **to** *vlan-id4* **stack-vlan** *vlan-id2* **remark-8021p** *priority*
- **no vlan-stacking all**
- **no vlan-stacking vlan** *vlan-id1*
- **no vlan-stacking vlan** *vlan-id1* **to** *vlan-id2*

Parameters

Parameters	Description	Value
vlan-id1	Specifies the first user VLAN ID to be mapped or indicates a single VLAN.	The value is an integer in the range from 1 to 4094.
vlan-id2	Specifies the outer VLAN ID tag.	The value is an integer in the

Parameters	Description	Value
		range from 1 to 4094.
vlan-id3	Specifies the batch user VLAN IDs to be mapped and indicates the first VLAN ID.	The value is an integer in the range from 1 to 4094.
vlan-id4	Specifies the batch user VLAN IDs to be mapped and indicates the last VLAN ID.	The value is an integer in the range from 1 to 4094.
priority	Specifies the 802.1p priority.	The value is an integer in the range from 0 to 7.

Default Value

None

View

Interface configuration view

Usage Guidelines

When a packet in this VLAN needs to traverse the carrier's network, you can use this command to add a VLAN tag to the packet to form a dual-layer VLAN.

Note the following when configuring the flexible QinQ:

- The interface must be a hybrid/trunk interface and is valid only in the inbound direction.
- The stacked outer VLAN must exist, and the current interface must be added to the stack VLAN in untagged mode.

Example

Configure the flexible QinQ function for interface 10GE1/0/1 and add an outer VLAN 20 tag to VLAN 2 packets.

```
switch(config-10ge1/0/1)#vlan-stacking vlan 2 stack-vlan 20
switch(config-10ge1/0/1)#
```

2.9.4 show vlan-stacking

Function

The **show vlan-stacking** command shows information about the flexible QinQ.

Format

- **show vlan-stacking**
- **show vlan-stacking config interface**
- **show vlan-stacking config interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **show vlan-stacking interface**
- **show vlan-stacking interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*

Parameters

Parameters	Description	Value

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer string in the range of <1-1>/<0-2>/<1-52>.

Default Value

None

View

Common user view, privileged user view, global configuration view and interface configuration view (Ethernet and trunk)

Usage Guidelines

None

Example

View information about flexible QinQ.

```
switch#show vlan-stacking
  Version                    :QINQ_VB3.00.02.00
  Max interface number       :332
  Max qinq items             :8192
  Current qinq items         :0
switch#
```

2.10 VLAN Mapping Configuration Commands

2.10.1vlan-mapping {enable|disable}

Function

The **vlan-mapping {enable|disable}** command enables or disables the interface VLAN mapping.

Format

- **vlan-mapping** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the interface VLAN mapping.	-
disable	Disables the interface VLAN mapping.	-

Default Value

Disable

View

Interface configuration view (Ethernet and trunk)

Usage Guidelines

None

Example

Enable the interface VLAN mapping.

```
switch(config-10ge1/0/1)#vlan-mapping enable
switch(config-10ge1/0/1)#
```

2.10.2 vlan-mapping vlan map-vlan

Function

The **vlan-mapping vlan map-vlan (remark-8021p)** command configures the 1:1 VLAN translation entries and matches the outer VLAN ID in a packet to modify the outer VLAN ID and priority.(Bidirectional mapping of VLAN tags, effective for known users)

The **vlan-mapping vlan to map-vlan (remark-8021p)** command configures the N:1 VLAN translation entries; that is, map multiple user VLAN ID tags to a network VLAN ID tag and matches the outer VLAN ID in a packet to modify the outer VLAN ID and priority.

The **vlan-mapping vlan inner-vlan map-vlan (remark-8021p)** command matches the outer VLAN ID and inner-layer VLANID of a data packet to modify the outer VLAN ID and priority, as well as matches the outer VLAN ID of a data packet to modify the outer VLAN ID and priority.(N8550-48b8c and N8550-32C do not support this feature.)

The **vlan-mapping vlan inner-vlan map-single-vlan** command matches the outer VLAN ID and maps it tothe specified VLANID of a new single-layer tag.(This feature only supports single-direction mapping of VLAN tags.)

The **no vlan-mapping all** command deletes all the configured VLAN mapping entries.

Format

- **vlan-mapping vlan** *outside-vlan-id* **map-vlan** *outside-mapping-vlan-id*
- **vlan-mapping vlan** *outside-vlan-id* **map-vlan** *outside-mapping-vlan-id* **remark-8021p** *priority*
- **vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner-vlan-id1* **to** *inner-vlan-id* 2 **map-vlan** *outside-mapping-vlan-id*
- **no vlan-mapping all**
- **no vlan-mapping vlan** outside-vlan-id **inner-vlan** *inner-mapping-vlan-id*
- **no vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner-mapping-vlan-id1* **to** *inner-mapping-vlan-id2*
- **no vlan-mapping vlan** *outside-vlan-id* **to** *outside-mapping-vlan-id*

Parameters

Parameters	Description	Value
outside-vlan-id	Specifies the outer-layer VLAN ID of a data packet.	The value is an integer in the range from 1 to 4094.
outside-mapping-vlan-id	Specifies the outer-layer VLAN ID of a translated data packet.	The value is an integer in the range from 1 to 4094.
priority	Specifies the VLAN priority.	The value is an integer in the range

Parameters	Description	Value
		from 0 to 7.
inner-vlan-id1 inner-vlan-id2	Specifies the inner-layer VLAN ID of a data packet.	The value is an integer in the range from 1 to 4094.
inner-mapping-vlan-id	Specifies the outer tag of a VLAN to which a port belongs. Inner VLAN IDs are mapped to this outer tag.	The value is an integer in the range from 1 to 4094.
inner--mapping-vlan-id1	Specifies the start value of multiple inner-layer VLAN IDs.	The value is an integer in the range from 1 to 4094.
inner--mapping-vlan-id2	Specifies the end value of multiple inner-layer VLAN IDs.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

Interface configuration view (Ethernet interface)

Usage Guidelines

The switch supports single-layer VLAN 1:1 mapping and N:1 mapping.

Example

Configure the VLAN translation entry.

```
switch(config-100ge1/0/1)#vlan-mapping vlan 10 map-vlan 100
switch(config-100ge1/0/1)#
```

2.10.3 show vlan-mapping

Function

The **show vlan-mapping** command shows the VLAN translation information, including configuration and interface information

Format

- **show vlan-mapping**
- **show vlan-mapping config**
- **show vlan-mapping interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*

Parameters

Parameters	Description	Value
10gigaethernet	Specifies a 10Gigabit Ethernet interface.	-
100gigaethernet	Specifies a 100Gigabit Ethernet interface.	-
interface-number	Specifies an Ethernet interface number.	The value is an integer string in the range of <1-1>/<0-2>/<1-52>.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet interface)

Usage Guidelines

None

Example

View VLAN translation information.

```
switch#show vlan-mapping
  Support Max Interface Number      :24
  Support Max Map List Number       :128
  Current Map List Number           :1
  Interface                Out-VID     Map-OutVID
  100gigaethernet 1/0/2    10/10       100
```

```
switch#show vlan-mapping config
 Interface 100gigaethernet 1/0/2
 vlan-mapping vlan 10 map-vlan 100

switch#show vlan-mapping interface 100gigaethernet 1/0/2
   Support Max Interface Number      :24
   Support Max Map List Number       :128
   Current Map List Number           :1
   Interface                 Out-VID     Map-OutVID
   100gigaethernet 1/0/2   10/10       100

switch#
```

2.11 Port Security Configuration Commands

2.11.1 Port Security Configuration Commands

2.11.2 port-isolate mode

Function

The **port-isolate mode** command configures Layer 2 or Layer 3 port isolation.

Format

- **port-isolate mode** { **l2** | **all** }

Parameters

Parameters	Description	Value
l2	Sets the port isolation mode to Layer 2 port isolation.	-
all	Sets the port isolation mode to both Layer 2 and Layer 3 isolation.	-

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Set the port isolation mode to Layer 2 port isolation.

```
switch(config)#port-isolate mode l2
switch(config)#
```

2.11.3 port-isolate group

Function

The **port-isolate group** command creates a port isolation group.

Format

- **port-isolate group** *group-number*

Parameters

Parameters	Description	Value
group-number	Specifies the number of a port isolation group.	The value is an integer in the range from 1 to 16.

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Create port isolation group 1.

```
switch(config)#port-isolate group 1
switch(config-isolate-group1)#
```

2.11.4 join port-isolate group

Function

The **join port-isolate group** command adds an interface to an isolation group.
The **no join port-isolate group** command removes an interface from an isolation group.

Format

- **join port-isolate group** *group-id*
- **join port-isolate group** *group-list*

- **no join port-isolate group** *group-id*
- **no join port-isolate group** *group-list*
- **no join port-isolate group all**

Parameters

Parameters	Description	Value
group-id	Specifies an isolation group ID.	The value is an integer in the range from 1 to 16.
group-list	Specifies an isolation group list ID. You can enter multiple VLAN IDs.	for example, 1, 3. Two VLAN IDs are separated by a comma (,) or hyphen (-). Two VLAN IDs with a hyphen identify a range of VLAN IDs.

Default Value

None

View

Interface configuration view

Usage Guidelines

This command adds an interface to a port isolation group. Interfaces in an isolation group can communicate with interfaces out of the isolation group but cannot communicate with interfaces in the same isolation group.

Example

Add interface 10gigaethernet1/0/1 to isolation group 4.

```
switch(config-100ge1/0/1)#join port-isolate group 4
switch(config-100ge1/0/1)#
```

2.11.5add interface

Function

The **add interface** command adds an interface to an isolation group.
The **no interface** command removes an interface from an isolation group.

Format

- **add interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **add interface eth-trunk** *trunk-number*
- **no interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **no interface eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of 1-1/0-2/1-52.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.

Default Value

None

View

Isolation group configuration view

Usage Guidelines

None

Example

Add interface 10gigaethernet1/0/1 to isolation group 1.

```
switch(config)#port-isolate group 1
switch(config-isolate-group1)#add interface 10gigaethernet 1/0/1
switch(config-isolate-group1)#
```

2.11.6show port-uniisolate interface

Function

The **show port-uniisolate interface** command displays the configuration of unidirectional port isolation.
The **show port-uniisolate online interface** command displays the configuration of all meaningful unidirectional port isolation.

Format

- **show port-uniisolate interface**
- **show port-uniisolate interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **show port-uniisolate interface eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of 1-1/0-2/1-52.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.

Default Value

None

View

Privileged user view, global configuration view, common user view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

The switch supports a maximum of 64 unidirectional port isolation groups.

Example

Display the configuration of unidirectional port isolation.

```
switch#show port-uniisolate interface
 uniisolate -port       being uniisolated-port
 10gigaethernet-1/0/1        10gigaethernet-1/0/2
switch#
```

2.11.7 show port-isolategroup

Function

The **show port-isolate group** command displays information about all or specified port isolation groups.

Format

- **show port-isolate group**
- **show port-isolate group** *group-number*

Parameters

Parameters	Description	Value
group-number	Specifies the number of a port isolation group.	The value is an integer in the range from 1 to 16.

Default Value

None

View

Privileged user view, global configuration view, common user view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

None

Example

Display information about port isolation group 2.

```
switch#show port-isolate group 2
```

```
The interfaces in isolate group 2:
--------------------------------------------------------------------------------
  10gigaethernet-1/0/1
switch#
```

2.11.8show port-isolate information

Function

The **show port-isolate information** command displays information about all port isolation groups.

Format

- **show port-isolate information**

Parameters

None

Default Value

None

View

Privileged user view, global configuration view, common user view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

None

Example

Display information about all port isolation groups.

```
switch#show port-isolate information
 Isolate Mode : l2Isolate
 Support Max Port Ioslate Group Count: 64
 Support Max Interface Count for Each Group : 705
 Current Used Interface-Group Node Count: 1
 Current Free Interface-Group Node Count: 45119
 Support Max Interface Count : 705
 Support Max Unidirectional Ioslate target Interface Count : 30
 Current Used Unidirectional-Ioslate Node Count: 0
 Current Used Bidirectional-Ioslate Node Count: 0
 Current Free Ioslate Node Count: 248160
switch#
```

2.11.9show port-isolate config

Function

The **show port-isolate config** command displays the configuration of an isolation group via configuration files.

Format

- **show port-isolate config**

Parameters

None

Default Value

None

View

Privileged user view, global configuration view, common user view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

None

Example

Display configuration of all port isolation groups.

```
switch#show port-isolate config
Version                         :PORTISOLATE_VB3.00.08.00
switch#
```

2.12 MVRP Configuration Command

2.12.1mvrp {start|stop}

Function

The **mvrp {start|stop}** command enables or disables the MVRP functional module globally.

Format

- **mvrp** { **start** | **stop** }

Parameters

Parameters	Description	Value
start	Enables the MVRP functional module globally.	-
stop	Disables the MVRP functional module globally.	-

Default Value

Stop

View

Global configuration view

Usage Guidelines

None

Example

Enable the MVRP functional module globally.

```
switch(config)#mvrp start
switch(config)#
```

2.12.2 mvrp gvrp-compliance {enable|disable}

Function

The **mvrp gvrp-compliance {enable|disable}** command enables or disables the GVRP compatibility globally.

Format

- **mvrp gvrp-compliance** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the GVRP compatibility globally.	-
disable	Disables the GVRP compatibility globally.	-

Default Value

disable

View

Global configuration view

Usage Guidelines

Enable GVRP first and then run this command.

Example

Enable the GVRP compatibility globally.

```
switch(config)#mvrp start
```

```
switch(config)#mvrp gvrp-compliance enable
```

2.12.3 mvrp {enable|disable}

Function

The **mvrp {enable|disable** command enables or disables the MVRP for an interface.

Format

- **mvrp** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the MVRP for an interface.	-
disable	Disables the MVRP for an interface.	-

Default Value

Disable

View

Interface configuration view (Ethernet, Trunk)

Usage Guidelines

Before using this command , run the **mvrp start** command to enable the MVRP globally. The port link type of an interface should be trunk. The interface should be pre-configured to allow the desired VLAN to pass.

Example

Enable the MVRP for an interface.

```
switch(config)#mvrp start
switch(config-100ge1/0/1)#port link-type trunk
switch(config-100ge1/0/1)#mvrp enable
```

2.12.4 mvrp timer leave

Function

The **mvrp timer leave** command sets the time-out time of the leave timer of the MVRP interface.

Format

- **mvrp timer leave** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	Specifies the time-out time of the Leave timer.	It is an integer ranging from 450-30000 (unit: ms)
default	Uses the default time-out time of the Leave timer.	30000 ms

Default Value

30000 ms

View

Interface configuration view (Ethernet, Trunk)

Usage Guidelines

To ensure the normal operation of MVRP, the correct value ranges of the Join timer, Leave timer and Leave-all timer are interdependent. If the value of a timer exceeds its current correct range, the configuration is error. You can reconfigure by modifying the value of the timer, which must be a multiple of 20 centiseconds. The time-out time of the Leave timer should be larger than twice the time-out time of the Join timer, and less than that of the Leave-all timer.

Example

Set the time-out time of the Leave timer to 20s.

```
switch(config)#mvrp start
switch(config)#interface 10gigaethernet 1/0/1
switch(config-10ge1/0/1)#mvrp enable
switch(config-10ge1/0/1)#mvrp timer leave 20000
switch(config-10ge1/0/1)#
```

2.12.5 mvrp timer leave-all

Function

The **mvrp timer leave-all** command sets the time-out time of the global leave-all timer for the MVRP interface.

Format

- **mvrp timer leave-all** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	Sets the time-out time of the global leave-all timer.	It is an integer ranging from 650 to 327650 (unit: ms).
default	Uses the default time-out time of the global leave-all timer.	120000 ms

Default Value

120000 ms

View

Interface configuration view (Ethernet, Trunk)

Usage Guidelines

To ensure the normal operation of MVRP, the correct value ranges of the Join timer, Leave timer and Leave-all timer are interdependent. If the value of a timer exceeds its current correct range, the configuration is error. You can reconfigure by modifying the value of the timer, which must be a multiple of 20 centiseconds. The time-out time of the Leave-all timer should be larger than the time-out time of the Leave timers on all ports.

Example

Set the time-out time of the global Leave-all timer to 100s.

```
switch(config)#mvrp start
switch(config)#interface 10gigaethernet 1/0/1
switch(config-100ge1/0/1)#mvrp enable
switch(config-100ge1/0/1)#mvrp timer leave-all 100000
switch(config-100ge1/0/1)#
```

2.12.6 mvrp timer join

Function

The **mvrp timer join** command sets the time-out time of the Join timer of an interface.

Format

- **mvrp timer join** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	Specifies the time-out time of the Join timer.	It is an integer ranging from 200 to 6000 (unit: ms).
default	Uses the default time-out time of the Join timer.	6000 ms

Default Value

6000 ms

View

Interface configuration view (Ethernet, Trunk)

Usage Guidelines

To ensure the normal operation of MVRP, the correct value ranges of the Join timer, Leave timer and Leave-all timer are interdependent. If the value of a timer exceeds its current correct range, the configuration is error. You can reconfigure by modifying the value of the timer, which must be a multiple of 20 centiseconds. The time-out time of the Join timer should be less than half the time-out time of the Leave timer.

Example

Sets the time-out time of the Join timer to 5s.

```
switch(config)#mvrp start
switch(config)#interface 10gigaethernet 1/0/1
switch(config-10ge1/0/1)#mvrp enable
switch(config-10ge1/0/1)# mvrp timer join 5000
```

2.12.7 mvrp registration

Function

The **mvrp registration** command configures the registration mode of the MVRP.

Format

- **mvrp registration** { **fixed** | **forbidden** | **normal** }

Parameters

Parameters	Description	Value
fixed	Fixed mode	-
forbidden	Forbidden mode	-
normal	Normal mode	-

Default Value

Normal

View

Interface configuration view (Ethernet, Trunk)

Usage Guidelines

Before using this command, run the **mvrp start** command to enable the MVRP globally.
There are three MVRP interface registration modes.

- Fixed mode: Forbids the dynamic interface registration and VLAN cancellation; transmits the static VLAN information rather than the dynamic VLAN information. That is, although a Trunk interface in Fixed mode allows all the VLANs to pass, only the VLANs configured manually can pass in practice.

- Forbidden mode: Forbids the dynamic interface registration and VLAN cancellation; Does not transmit the any VLAN information except the VLAN1 information. That is, although a Trunk interface in Forbidden mode allows all the VLANs to pass, only the VLAN1 can pass in practice.
- Normal mode: Allows the dynamic interface registration and VLAN cancellation; transmits both the static and dynamic VLAN information.

Example

Configure the MVRP registration mode.

```
switch(config)#mvrp start
switch(config)#interface 10gigaethernet 1/0/1
switch(config-10ge1/0/1)#mvrp enable
switch(config-10ge1/0/1)#mvrp registration fixed
switch(config-10ge1/0/1)#
```

2.12.8 show mvrp

Function

The **show mvrp** command displays the MVRP configuration.

Format

- **show mvrp**
- **show mvrp interface** { **10gigaethernet** | **100gigaethernet** } *interface-number* **vlan** *vlan-id*
- **show mvrp interface eth-trunk** *trunk-number* **vlan** *vlan-id*

Parameters

Parameters	Description	Value
interface-number	Specifies the Ethernet interface number.	It is an integer . The values include <1-1> / <0-2> / <1-52>.
trunk-number	Specifies the Trunk interface number.	It is an integer ranging from 1 to 32.
vlan-id	Specifies the VLAN ID	It is an integer raging from 1 to 4094.

Default Value

None

View

Priviledge user view, global configuration view and interface configuration view (Ethernet, Trunk)

Usage Guidelines

None

Example

View the MVRP configuration.

```
switch#show mvrp interface 10gigaethernet 1/0/1 vlan 1
                Mvrp status:        enable
                Join timer:         225ms
                Leave timer:        750ms
                LeaveAll timer:     3000ms
                Periodic timer:     5000ms
                Registration type:     fixed
switch#show mvrp
Mvrp general informaiton:
          mvrp:        enable
          Compliance-GVRP:       disable
Mvrp interface information:
Interface:10 ge-1/0/1
             Mvrp status:       enable
             Join timer:         225ms
             Leave timer:       750ms
             LeaveAll timer:     3000ms
             Periodic timer:       5000ms
             Registration type:       fixed
Interface: 10ge-1/0/2
             Mvrp status:       enable
             Join timer:         200ms
             Leave timer:       600ms
             LeaveAll timer:     10000ms
             Periodic timer:       1000ms
             Registration type:       normal
--More--
```

2.13 PVLAN Configuration Commands

This section introduces the private-VLAN-related configuration commands.

2.13.1no private-vlan

Function

The **no private-vlan** command restores a private VLAN to common VLAN.

Format

- **no private-vlan**

Parameters

None

Default Value

None

View

VLAN configuration view

Usage Guidelines

If you do not need the private VLAN function, you can use this command to restore it to a common VLAN.
PVLAN cannot interact with common VLAN.

Example

Restore VLAN 3 in private-vlan to a common VLAN.

```
switch(config-vlan-3)#no private-vlan
switch(config-vlan-3)#
```

2.13.2 private-vlan association {add|remove}

Function

The **private-vlan association add** command associates a primary VLAN with a secondary VLAN.
The **private-vlan association remove** command removes the association between a primary VLAN and all its secondary VLANs.

Format

- **private-vlan association** { **add** | **remove** } *vlan-list*

Parameters

Parameters	Description	Value
add	Configures the association between a list of secondary VLANs and a primary VLAN.	-
remove	Removes the association between a list of secondary VLANs and a primary VLAN.	-
vlan-list	Specifies a list of secondary VLANs. Continuous VLANs are the starting VLAN and ending VLAN connected by "-". Discontinuous VLANs are separated by ",".	1-4094

Default Value

None

View

VLAN configuration view

Usage Guidelines

None

Example

Associate a list of secondary VLANs (VLAN 12-VLAN 14) and a primary VLAN10.

```
switch(config-vlan-10)#private-vlan association add 12-14
switch(config-vlan-10)#
```

2.13.3 private-vlan association

Function

The **private-vlan association** command configures a primary VLAN and the associated secondary VLAN.
The **no private-vlan association** command removes the primary VLAN and the associated secondary VLAN.

Format

- **private-vlan association** *vlan-list*
- **vlan** *vlan-id* **private-vlan association** *vlan-list*
- **no private-vlan association**

Parameters

Parameters	Description	Value
vlan-id	Specifies a primary VLAN ID.	The value is an integer in the range from 1 to 4094.
vlan-list	Specifies a list of secondary VLAN IDs.	The value is in the range from 1 to 4094, for example, 10, 20, and 30-32.

Default Value

None

View

VLAN configuration view

Usage Guidelines

None

Example

Configure the list of the secondary VLANs associated to primary VLAN3 to VLAN 20 and VLAN30.

```
switch(config-vlan-3)#private-vlan association 20,30
```

```
switch(config-vlan-3)#
```

2.13.4 private-vlan host-association

Function

The **private-vlan host-association** command associates a host port with the primary VLAN and secondary VLAN.
The **no private-vlan host-association** command removes the association between a host port and the primary VLAN and secondary VLAN.

Format

- **private-vlan host-association** *vlan1 vlan2*
- **no private-vlan host-association** *vlan1 vlan2*

Parameters

Parameters	Description	Value
vlan1	Specifies the primary VLAN.	The value is an integer in the range from 1 to 4094.
vlan2	Specifies the secondary VLAN.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

Interface configuration view (Ethernet and trunk)

Usage Guidelines

Before using this command, set the port to the host mode and set the association between the primary VLAN and the secondary VLAN.

Example

Associate interface gigaethernet1/0/1 with primary VLAN 2 and secondary VLAN 3.

```
switch(config-100ge1/0/1)#private-vlan host-association 2 3
switch(config-100ge1/0/1)#
```

2.13.5 private-vlan mapping

Function

The **private-vlan mapping** command establishes the association between promiscuous port and primary/secondary VLAN.

Format

- **private-vlan mapping** *vlan-id* { **add** | **remove** } *vlan-list*

Parameters

Parameters	Description	Value
vlan-id	Specifies the primary VLAN.	The value is an integer in the range from 1 to 4094.
vlan-list	Specifies the secondary VLAN.	-

Default Value

None

View

Interface configuration view (Ethernet and trunk)

Usage Guidelines

You can use this command only after you configure a port as a promiscuous port using the private-vlan modecommand.

Example

Establish the association between interface gigaethernet1/0/1 and primary VLAN10 and secondary VLAN2.

```
switch(config-100ge1/0/1)#private-vlan mapping 10 add 2
switch(config-100ge1/0/1)#
```

2.13.6 private-vlan mode

Function

The **private-vlan mode** command configures the mode of all private VLAN interfaces.

Format

- **private-vlan mode** { **native** | **host** | **promiscuous** }

Parameters

Parameters	Description	Value
native	Specifies the non-private VLAN mode.	-
host	Specifies the host mode.	-
promiscuous	Specifies the promiscuous mode.	

Default Value

None

View

Interface configuration view (Ethernet and trunk)

Usage Guidelines

The PVLAN interfaces include two types: promiscuous interfaces and host interfaces.
Host mode: The port belongs to a secondary VLAN and inherits attributes of the secondary VLAN. Host interfaces are classified into isolation interfaces and communication interfaces.
Promiscuous mode: The port belongs only to the primary VLAN.

Example

Configure a private VLAN interface as a promiscuous interface.

```
switch(config-100ge1/0/1)#private-vlan mode promiscuous
switch(config-100ge1/0/1)#
```

2.13.7 private-vlan {primary|isolated|community}

Function

The **private-vlan {primary|isolated|community}** command configures the private VLAN mode.

Format

- **private-vlan** { **primary** | **isolated** | **community** }
- **vlan** *vlan-id* **private-vlan** { **primary** | **isolated** | **community** }

Parameters

Parameters	Description	Value
primary	Specifies a primary VLAN.	-
isolated	Specifies an isolated VLAN.	-
community	Specifies a communication VLAN.	-

Default Value

None

View

VLAN configuration view, global configuration view

Usage Guidelines

One primary VLAN can be associated with only one isolated VLAN.
One promiscuous port can be associated with only one primary VLAN.
One isolated port can be associated with only one secondary VLAN.
One community port can be associated with only one secondary VLAN.

One secondary VLAN can be associated with only one primary VLAN.
Each PVLAN includes only one primary VLAN.
Multiple PVLANs can co-exist on one switch or one switched network.

Example

Configure the private VLAN as the primary VLAN.

```
switch(config-vlan-1)#private-vlan primary
switch(config-vlan-1)#
```

2.13.8 private-vlan primary-vid

Function

The **private-vlan primary-vid** command associates a secondary VLAN with a primary VLAN.

Format

- **private-vlan primary-vid** *vlan-id*

Parameters

Parameters	Description	Value
vlan-id	Specifies the to-be-associated primary VLAN ID.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

VLAN configuration view

Usage Guidelines

You can associate only one secondary VLAN with a primary VLAN when using this command.

Example

Associate secondary VLAN 2 with primary VLAN 10.

```
switch(config-vlan-2)#private-vlan primary-vid 10
switch(config-vlan-2)#
```

2.13.9 show private-vlan interface

Function

The **show private-vlan interface** command shows the interface mode and the associated secondary VLAN information.

Format

- **show private-vlan interface**

Parameters

None

Default Value

None

View

Privileged user view, global configuration view, common user view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

You can use this command to view the interface ID, mode, and associated secondary VLAN.

Example

View information about interfaces in a private VLAN.

```
switch#show private-vlan interface
Interface     Type            Primary   Secondary
100ge1/0/1    host              20          3
switch#
```

2.13.10 show private-vlan mapping

Function

The **show private-vlan mapping** command shows information of a private VLAN.

Format

- **show private-vlan mapping**

Parameters

None

Default Value

None

View

Privileged user view, global configuration view, common user view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

The command output includes the primary VLAN, secondary VLAN, and type of the secondary VLAN.

Example

View the information about a private VLAN.

```
switch#show private-vlan mapping
Primary   Sencondary   Type
10            2            isolated
switch#
```

3. IP Commands

3.1 Overview

This chapter introduces the IP address configuration commands of the N-series switch.

3.2 IPv4 Address Configuration Commands

3.2.1 ip address

Function

The **ip address** command configures an IP address for VLAN interface.
The **no ip address** command deY IP addresses or an IP address for VLAN interface.

Format

- **ip address** *ip-address/mask-length*
- **ip address** *ip-address mask-address*
- **no ip address** *ip-address*
- **no ip address**

Parameters

Parameters	Description	Value
ip-address	Specifies the IP address of the interface.	The value is in dotted decimal notation.
mask-address	Specifies the mask address.	The value is in dotted decimal notation.
ip-address/ mask-length	Specifies the IP address and mask address.	The value is in dotted decimal notation. Mask-length indicates the length of the mask address. The value is an integer ranging from 1 to 32.

Default Value

By default, no IP address is configured in each VLAN view.

View

VLANIF configuration view, Tunnel interface configuration view, and Loopback interface configuration view

Usage Guidelines

This command assigns an IP address and mask to a VLAN interface to ensure network connectivity.

Note: The switch does not support IP address configuration on 10GE, 100GE or trunk interfaces.
All IP addresses configured for each interface cannot be in the same subnet.

Example

Set the primary IP address to 10.18.13.20 in the VLAN 3 view and subnet mask length to 24.

```
switch(config-vlanif-3)#ip address 10.18.13.20/24
switch(config-vlanif-3)#
```

3.2.2 mtu

Function

The **mtu** command configures the MTU size of an IPv4 interface.

Format

- **mtu** { *mtu-value* | **default** }

Parameters

Parameters	Description	Value
mtu-value	Specifies the MTU size.	The value is an integer. In the VLANIF configuration view, the value ranges from 128 to 9216. The default is 1500 bytes. The value is an integer. In the Tunnel interface configuration view, the value ranges from 64 to 9728. The default is 1522 in bytes .

Default Value

In the VLANIF configuration view, the default is 1500.
In the Tunnel configuration view, the default is 1522.

View

VLANIF configuration view and Tunnel interface configuration view

Usage Guidelines

None

Example

Set the MTU value to 1400.

```
switch(config-vlanif-2)#mtu 1400
switch(config-vlanif-2)#
```

3.2.3 ip prefix-list

Function

The **ip prefix-list** command configures an IPv4 prefix list.
The **no ip prefix-list** command cancels the configuration.

Format

- **ip prefix-list** *list-name* { **deny** | **permit** } *ipv4-address/mask-length*
- **ip prefix-list** *list-name* { **deny** | **permit** } *ipv4-address/mask-length* { **greater-equal** | **less-equal** } *prefix-length*
- **ip prefix-list** *list-name* { **deny** | **permit** } *ipv4-address/mask-length* **greater-equal** *prefix length* **less-equal** *prefix-length*
- **ip prefix-list** *list-name* **index** *index-number* { **deny** | **permit** } *ipv4-address/mask-length*
- **ip prefix-list** *list-name* **index** *index-number* { **deny** | **permit** } *ipv4-address/mask-length* { **greater-equal** | **less-equal** } *prefix-length*
- **ip prefix-list** *list-name* **index** *index-number* { **deny** | **permit** } *ipv4-address/mask-length* **greater-equal** *prefix length* **less-equal** *prefix-length*
- **no ip prefix-list** *list-name*
- **no ip prefix-list** *list-name* **index** *index-number*

Parameters

Parameters	Description	Value
list-name	Specifies the name of a prefix list.	-
deny|permit	Specifies the action of allowing or rejecting a packet with the IP address in the list.	-
ipv4-address	Specifies an IPv4 address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of an IPv4 address.	The value is an integer in the range from 0 to 32.
greater-equal|less-equal	Specifies an action taken when the length of a prefix is no longer than or no shorter than the length of the IPv4 address prefix.	-
prefix-length	Specifies the prefix length.	The value is an integer in the range from 0 to 32.
index	Specifies the index.	-
index-number	Specifies the index number.	The value is an integer in the range from 1 to 65535.

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Configure the action of permitting entry 123 with IPv4 address 10.10.10.10, mask length 24, and prefix of no shorter than 20.

```
switch(config)#ip prefix-list 123 permit 10.10.10.10/24 greater-equal 20
switch(config)#
```

3.2.4 ip forward-strict {enable|disable}

Function

The **ip forward-strict {enable|disable}** command enables or disables strict layer 3 IP forwarding.

Format

- **ip forward-strict** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables strict layer 3 IP forwarding.	-
disable	Disables strict layer 3 IP forwarding.	-

Default Value

disable

View

Global configuration view

Usage Guidelines

None

Example

Enable strict layer 3 IP forwarding.

```
switch(config)#ip forward-strict enable
switch(config)#
```

3.2.5 icmp redirect send {enable|disable}

Function

The **icmp redirect send {enable|disable}** command enables or disables the sending of ICMP redirect packets. (This command applies to IPv4 networks.)

Format

- **icmp redirect send** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the sending of ICMP redirect packets.	-
disable	Disable the sending of ICMP redirect packets.	-

Default Value

disable

View

VLANIF configuration view

Usage Guidelines

This command is available to administrators.

Example

Enable the sending of ICMP redirect packets.

```
switch(config-vlanif-3)#icmp redirect send enable
switch(config-vlanif-3)#
```

3.2.6 show ip interface

Function

The **show ip interface** command displays IPv4 interface information.

Format

- **show ip interface**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, and VLANIF configuration view

Usage Guidelines

None

Example

Display the IPv4 interface information.

```
switch#show ip interface
  The total number of ip address: 2
  Ip-Address      Interface          IPIndex State(a/o)  Role          Type
  10.18.16.19/24  vlan-3             1       up/down     primary       static
  127.0.0.1/8     loopback-0         2       up/up       primary       auto

switch#
```

3.2.7 show ip statistic

Function

The **show ip statistic** command displays IP statistics.

Format

- **show ip statistic**
- **show ip tcp statistic**
- **show ip udp statistic**
- **show ip icmp statistic**
- **show ip connect-table**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

The IP statistics include IP information, TCP information, UDP information, ICMP information, IGMP information, and TCP/UDP connection table information.

Example

Check IP statistics.

3.3 DHCP Configuration Commands

3.3.1 dhcp {start|stop}

Function

The **dhcp {start|stop}** command enables or disables the DHCP function on the switch.

Format

- **dhcp** { **start** | **stop** }

Parameters

Parameters	Description	Value
start	Enables the DHCP function.	-
stop	Disables the DHCP function.	-

Default Value

By default, the DHCP function is disabled.

View

Global configuration view

Usage Guidelines

You can use this command to enable the DHCP function. This command must be executed before all the other DHCP configuration commands. Other DHCP attribute configurations can take effect only after the DHCP function is enabled.

Example

Enable the DHCP function.

```
switch(config)#dhcp start
switch(config)#
```

3.3.2 dhcp address-check-time

Function

The **dhcp address-check-time** command configures the conflict time detected of the DHCP address detection.

Format

- **dhcp address-check-time** { *check-time* | **default** }

Parameters

Parameters	Description	Value

Parameters	Description	Value
check-time	Specifies the conflict time of the address detection.	The value is an integer ranging from 0 to 10000, in milliseconds.
default	Specifies the Default Value.	The value is 500 ms.

Default Value

By default, the conflict time of DHCP address detection is set to 500 ms.

View

Global configuration view

Usage Guidelines

If the maximum conflict time of address detection is set to 0, address detection is not performed.

Example

Set the conflict time of DHCP address detection to 1000 ms.

```
switch(config)#dhcp address-check-time 1000
switch(config)#
```

3.3.3 option

Function

The **option** command configures the attribute value of the DHCP user-defined option.
The **no option** command deletes the attribute value of the DHCP user-defined option.

Format

- **option** *option1-range* **ip-address** *ip-address*
- **option** *option2-range* **ascii** *ascii-string*
- **option** *option3-range* **hex** *hex-string*
- **no option** *option4-range*

Parameters

Parameters	Description	Value
option1-range	Specifies the option range.	The value is an integer ranging from 2 to 254.
option2-range	Specifies the option range.	The value is an integer ranging from 2 to 254.
option3-range	Specifies the option range.	The value is an integer ranging from 2 to 254. Option 212 is not configured using this command.

Parameters	Description	Value
option4-range	Specifies the option range.	The value is an integer ranging from 2 to 254.
ip-address	Set the type of option60 to the IP address.	The value is in dotted decimal notation.
ascii-string	Set the type of option60 to the ASCII character string.	The value is a string of 1 to 127 characters.
hex-string	Set the type of option60 to the hexadecimal character string.	The character string must be an even number in hexadecimal format (HH or HHHH).

Default Value

None

View

DHCP Pool configuration view

Usage Guidelines

The Option field in the DHCP packet saves control information and Parameters that are not defined in common protocols. If the Option field is configured on the DHCP server, when a DHCP client applies for an IP address, it can obtain the configuration of the Option field through the responded DHCP packets. The DHCP uses the Option field to transfer control information and network configuration Parameters, and therefore providing more network configuration information to the clients.

Example

Set the Option to ASCII character string feisu.

```
switch(config-dhcp-pool-1)#option 11 ascii feisu
switch(config-dhcp-pool-1)#
```

3.3.4 option sub-option

Function

The **option sub-option** command configures the attribute value of a sub-option in a DHCP user-defined option.
The **no option sub-option** command deletes the attribute value of a sub-option in a DHCP user-defined option.

Format

- **option** *option-range* **sub-option** *sub-option* **ip-address** *ip-address*
- **option** *option-range* **sub-option** *sub-option* **ascii** *ascii-string*
- **option** *option-range* **sub-option** *sub-option* **hex** *hex-string*
- **no option** *option-range* **sub-option** *sub-option*

Parameters

Parameters	Description	Value
option-range	Specifies the option range.	The value is an integer from 2 to 254.
sub-option	Specifies the sub-option range.	The value is an integer from 1 to 254.
ip-address	Specifies the IPv4 address of a sub-option.	The value is in dotted notation
ascii-string	Set the type of a sub-option to the ASCII character string.	The value is a string of 1 to 127 characters
hex-string	Set the type of a sub-option to the hexadecimal character string.	The character string must be an even number in hexadecimal format (HH or HHHH).

Default Value

None

View

DHCP Pool configuration view

Usage Guidelines

None

Example

Set the sub-option in Option to ASCII character string feisu.

```
switch(config-dhcp-pool-1)#option 11 sub-option 2 ascii feisu
switch(config-dhcp-pool-1)#
```

3.3.5 option ipv6 rd ipv4 prefix-len prefix br

Function

The **option ipv6 rd ipv4 prefix-len prefix br** command configures the hex string value of option212.

Format

- **option ipv6 rd ipv4 prefix-len** *len-range* **prefix** *ipv6-address/MASK* **br** *ivp4-address*

Parameters

Parameters	Description	Value

Parameters	Description	Value
len-range	ip address mask length	integer, 0-32
ipv6-address/MASK	IPv6 addres prefix and its length	IP address with 128 bits is separated into 8 groups, 16 bits for each group are represented as 4 hexadecimal strings (0-9, A-F). Groups are separated with colon (:). In those hexadecimals, each 'X' indicates a group of hexadecimal number.
ivp4-address	IPv4 address	dotted decimal

Default Value

None

View

DHCP Pool Configuration View

Usage Guidelines

None

Example

Configure the hexadecimal character string of the option212.

```
switch(config-dhcp-pool-1)#option ipv6 rd ipv4 prefix-len 24 prefix 2001::1/24 br 10.18.2.12
switch(config-dhcp-pool-1)#
```

3.3.6 dhcp option82 circuit-id

Function

The **dhcp option82 circuit-id** command configures the sub-option Circuit ID of DHCP Option 82.
The **no dhcp option82 circuit-id** command deletes the sub-option Circuit ID of DHCP Option 82

Format

- **dhcp option82 circuit-id** *circuited*
- **dhcp option82 circuit-id format user-defined** *txt*
- **no dhcp option82 circuit-id**

Parameters

Parameters	Description	Value
circuitid	Specifies the sub-option Circuit ID of the DHCP relay option.	The value is a character string.
txt	Specifies the user-defined sub-option Circuit ID of	The value is a character string.

Parameters	Description	Value
	DHCP Option 82.	

Default Value

By default, the sub-option Circuit ID of DHCP Option 82 is not configured for the DHCP relay.

View

VLANIF configuration view

Usage Guidelines

The DHCP Option 82 can contain up to 255 sub-options. If DHCP Option 82 is enabled, you must define at least one sub-option. Currently, sub-option 1, sub-option 2, and sub-option 9 of DHCP Option 82 are commonly used.
Sub-option 1 is a sub-option of Option 82 and is the sub-option of the Circuit ID option. Generally, this sub-option is configured on the DHCP relay device. By default, it defines that packets must carry the VLAN ID and layer-2 port number of the switch port connected to the DHCP client. Generally, sub-option 1 and sub-option 2 identify the DHCP source end together.

Example

#Set the sub-option of the Circuit ID option to feisu.

```
switch(config-vlanif-3)#dhcp option82 circuit-id feisu
switch(config-vlanif-3)#
```

3.3.7 dhcp option82 {enable|disable}

Function

The **dhcp option82 {enable|disable}** command enables or disables the Option 82 function of the DHCP relay.

Format

- **dhcp option82** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables DHCP relay support for Option 82.	-
disable	Disables DHCP relay support for Option 82.	-

Default Value

By default, the DHCP relay does not support the Option 82 function.

View

VLANIF configuration view

Usage Guidelines

Option 82 must work in DHCP relay mode. You must run the ip dhcp command to enable the DHCP to work in relay mode. Option 82 is the relay agent information option in a DHCP packet. W hen a DHCP client sends a request packet to the DHCP server, the DHCP relay adds Option 82 to the request packet if the packet needs to pass through the DHCP relay. Option 82 achieves the function of recording address information of the DHCP client and DHCP relay on the DHCP server. It can cooperate with other software to implement DHCP allocation limit and charging.

Note: After the DHCP relay support for Option 82 is enabled, the switch adopts the keep policy to process Option 82-carried request packet. If other processing policies are enabled before the DHCP relay support for Option 82 is enabled, the processing policy is restored to the default after you enable the DHCP relay support for Option 82.

Example

Enable DHCP relay support for Option 82.

```
switch(config-vlanif-3)#dhcp option82 enable
switch(config-vlanif-3)#
```

3.3.8 dhcp option82 {drop|keep|replace}

Function

The **dhcp option82 {drop|keep|replace}** command configures the policy of the DHCP relay for processing the Option 82-carried request packet sent by the DHCP client.

Format

- **dhcp option82** { **drop** | **keep** | **replace** }

Parameters

Parameters	Description	Value
drop	If the packet carries Option 82, the switch drops the packet.	-
keep	If the packet carries Option 82, the，switch remains Option 82 unchanged and forwards the packet.	-
replace	If the packet carries Option 82, the switch fills in Option 82 according to the configuration to replace the original content, and forwards the packet.	-

Default Value

The default is keep.

View

VLANIF configuration view

Usage Guidelines

You can use this command to configure the policy for processing Option 82-carried request packets sent by a DHCP client for the DHCP relay.

Example

Set the policy for processing Option 82-carried request packets sent by a DHCP client for the DHCP relay to drop.

```
switch(config-vlanif-3)#dhcp option82 drop
switch(config-vlanif-3)#
```

3.3.9 dhcp option82 remote-id

Function

The **dhcp option82 remote-id** command configures the sub-option Remote ID of DHCP Option 82.
The **no dhcp option82 remote-id** command deletes the sub-option Remote ID of DHCP Option 82.

Format

- **dhcp option82 remote-id** *remoteid*
- **dhcp option82 remote-id format user-defined** *txt*
- **no dhcp option82 remote-id**

Parameters

Parameters	Description	Value
remoteid	Specifies the content of user-defined sub-option Remote ID. By default, Remote ID carries the MAC address of the switch. If you configure the content of this sub-option using the command line, the Remote ID content in the Option 82 becomes the configured content.	The value is a case-sensitive character string.
txt	Indicates the sub-option Remote ID of the user-defined DHCP Option 82.	The value is a character string.

Default Value

By default, the Remote ID of DHCP Option 82 is not configured for the DHCP relay.

View

VLANIF configuration view

Usage Guidelines

The DHCP Option 82 can contain up to 255 sub-options. If DHCP Option 82 is enabled, you must define at least one sub-option. Currently, sub-option 1, sub-option 2, and sub-option 9 of DHCP Option 82 are commonly used.
Sub-option 2 is a sub-option of Option 82 and is the sub-option of the Remote ID option. Generally, this sub-option is configured on the DHCP relay and defines the MAC address that needs to be carried in the packets. Generally, sub-option 2 and sub-option 1 identify the DHCP source end together.

Example

Set the content of sub-option Remote ID to feisudevice1.

```
switch(config-vlanif-3)#dhcp option82 remote-id feisudevice1
switch(config-vlanif-3)#
```

3.3.10 dhcp pool

Function

The **dhcp pool** command creates a DHCP address pool and enters the DHCP pool configuration view.
The **no dhcp pool** command deletes a created DHCP address pool.

Format

- **dhcp pool** *pool-number*
- **no dhcp pool** *pool-number*

Parameters

Parameters	Description	Value
pool-number	Specifies the address pool number.	The value is an integer ranging from 1 to 64.

Default Value

None.

View

Global configuration view

Usage Guidelines

You can use this command to create an IP address pool and manage Parameters such as NMS and rental period. This address pool is used to allocate addresses to DHCP servers.

Example

Create DHCP address pool 12 and access the address pool configuration view.

```
switch(config)#dhcp pool 12
switch(config-dhcp-pool-12)#
```

3.3.11dhcp relay server-ip

Function

The **dhcp relay server-ip** command configures the IP address of the DHCP server proxied by the DHCP relay.
The **no dhcp relay server-ip** command deletes the IP address of the DHCP relay server.

Format

- **dhcp relay server-ip** *ip-address*
- **no dhcp relay server-ip** *ip-address*

Parameters

Parameters	Description	Value
ip-address	Specifies the IP address of the DHCP server proxied by the DHCP relay.	The value is in dotted decimal notation.

Default Value

By default, the IP address of the DHCP server proxied by the DHCP relay is not configured.

View

VLANIF configuration view

Usage Guidelines

When the switch functions as a DHCP relay, after you configure the IP address of the DHCP server proxied by the DHCP relay using this command, the interface forwards DHCP broadcast request packets received from DHCP clients to the proxied DHCP server, and therefore achieving the cross-network segment DHCP service

Example

Configure the IP address of the DHCP server proxied by the DHCP relay.

```
switch(config-vlanif-3)#dhcp relay server-ip 10.16.13.23
switch(config-vlanif-3)#
```

3.3.12 dhcp relay static-bind

Function

The **dhcp relay static-bind** command configures the static user address binding entry of the DHCP relay (you can specify a VPN instance).
The **no dhcp relay bind** command deletes a static user address binding entry on the DHCP relay.

Format

- **dhcp relay static-bind** *ip-address mac-address*
- **no dhcp relay bind** *ip-address*
- **no dhcp relay bind all**

Parameters

Parameters	Description	Value
ip-address	Specifies the IP address of a DHCP client.	The value is in dotted decimal notation.
mac-address	Specifies the MAC address of a DHCP client.	The value is in the AA:BB:CC:DD:EE:FF format, where each of the letters A to F represents a hexadecimal digit.

Default Value

By default, the static user address binding entry of the DHCP relay is not configured.

View

Global configuration view

Usage Guidelines

You can use this command to configure the static user address binding entry of the DHCP relay, that is, the static binding between an IP address and a MAC address.

Example

Set the client IP address to 10.18.11.2 and MAC address to 00:00:00:ee:ff:ab in the static user address binding entry of the DHCP relay.

```
switch(config)#dhcp relay static-bind 10.18.11.2 00:00:00:ee:ff:ab
switch(config)#
```

3.3.13 dhcp relay user refresh-interval

Function

The **dhcp relay user refresh-interval** command configures the scheduled update period for the DHCP relay user table entry.

Format

- **dhcp relay user refresh-interval** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	Configures the scheduled update period for the DHCP relay user table entry	The value is an integer ranging from 60 to 3600, in seconds.

Parameters	Description	Value
default	Sets the scheduled update period for the DHCP relay user table entry to the Default Value value.	1800 seconds

Default Value

By default, the scheduled update period for the DHCP relay user table entry is set to 1800s.

View

Global configuration view

Usage Guidelines

You can use this command to set the update period for the DHCP relay user table entry or the default update period.

Example

Set the update period for the DHCP relay user table entry to 600s.

```
switch(config)#dhcp relay user refresh-interval 600
switch(config)#
```

3.3.14 dhcp server detect

Function

The **dhcp server detect** command enables or disables detection of pseudo DHCP servers.

Format

- **dhcp server detect** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables detection of pseudo DHCP servers.	-
disable	Disables detection of pseudo DHCP servers.	-

Default Value

By default, detection of pseudo DHCP servers is disabled.

View

Global configuration view

Usage Guidelines

In case there is a DHCP server secretly set up in the network, when a client applies for the IP address, this DHCP server interacts with the DHCP client, which causes the client to obtain the incorrect IP address. This kind of DHCP server is called the pseudo DHCP server.

You can use this command to disable detection of pseudo DHCP servers.

Once the pseudo DHCP server detection function is enabled, when the DHCP client sends the DHCP Request packets, the DHCP server obtains the IP address of the server that allocates the IP address to the client and records this IP address and the interface receiving the message. This provides convenience for the administrator to detect and handle the pseudo DHCP server in time.

Example

Enable detection of pseudo DHCP servers.

```
switch(config)#dhcp server detect enable
switch(config)#
```

3.3.15 dhcp server forbidden-ip

Function

The **dhcp server forbidden-ip** command configures IP addresses in the DHCP address pool that are not automatically allocated.

The **no dhcp server forbidden-ip** command cancels the IP addresses in the DHCP address pool that are not automatically allocated.

Format

- **dhcp server forbidden-ip** *ip-address1* [*ip-address2*]
- **no dhcp server forbidden-ip** *ip-address1* [*ip-address2*]

Parameters

Parameters	Description	Value
ip-address1	Specifies the minimum IP address that does not automatically allocated.	The value is in dotted decimal notation.
[ip-address2]	Specifies the maximum IP address that does not automatically allocated. The value cannot be smaller than ip-address1. If this Parameters is not specified, only one IP address exists.	The value is in dotted decimal notation.

Default Value

By default, except for the IP address of the DHCP server interface, all IP addresses in the DHCP address pool are automatically allocated.

View

DHCP Pool configuration view

Usage Guidelines

If an IP address is bound as a static IP address, it cannot be excluded.
If an IP address is excluded, it cannot be bound as a static IP address.
If IP addresses in a certain address range are not automatically allocated, you can cancel a certain IP address when canceling the exclusion.

Example

Reserve IP addresses from 10.18.16.1 to 10.18.16.50.

```
switch(config-dhcp-pool-1)#dhcp server forbidden-ip 10.18.16.1 10.18.16.50
switch(config-dhcp-pool-1) #
```

3.3.16 dhcp server option82

Function

The **dhcp server option82** command enables or disables the Option 82 function of the DHCP server.

Format

- **dhcp server option82** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the DHCP server to support the Option82 function.	-
disable	Disables the DHCP server to support the Option82 function.	-

Default Value

By default, the DHCP server supports the Option82 function.

View

Global configuration view

Usage Guidelines

The Options field in the DHCP packet saves control information and Parameters that are not defined in common protocols. The Options field consists of Code, Length, and Value. Option82 indicates an Options field with Code set to 82.

If the DHCP server is configured to support the Option82 function, the DHCPREPLY packet includes the Option82 content when the DHCP server receives a DCHP request carrying Option82. Otherwise, the Option82 content is not included. Address allocation to the DHCP clients by the DHCP server is not affected regardless of whether the Option 82 function is enabled.

Example

Enable the DHCP server to support the Option 82 function.

```
switch(config)#dhcp server option82 enable
switch(config)#
```

3.3.17 dhcp server static-bind

Function

The **dhcp server static-bind** command binds an IP address in the DHCP address pool with an MAC address. The VPN instance can be specified during binding.
The **no dhcp server static-bind** command cancels the binding between an IP address in the DHCP address pool and an MAC address.

Format

- **dhcp server static-bind** *ip-address mac-address*
- **no dhcp server static-bind** *ip-address*

Parameters

Parameters	Description	Value
ip-address	Specifies a bound IP address. It must be a valid IP address in the address pool.	The value is in dotted decimal notation.
mac-address	Specifies the MAC address.	The value is in the AA:BB:CC:DD:EE:FF format, where A-F is an hexadecimal number.

Default Value

By default, no IP address is bound with the MAC address of a user.

View

Global configuration view

Usage Guidelines

When a user requires a fixed IP address, you can run this command to bind an idle IP address in the address pool with the user's MAC address. After binding, the IP address exists permanently without rental time limitation. W hen the user uses this IP address, the configuration cannot be deleted.
If the IP address is unbound, the IP address becomes an idle IP address. Other users can apply for this IP address.

Example

Bind MAC address 00:00:00:aa:bb:cc with IP address 10.18.16.100 in the address pool.

```
switch(config)#dhcp server static-bind 10.18.16.100 00:00:00:aa:bb:cc
switch(config)#
```

3.3.18 dns

Function

The **dns** command configures the IP address of the DHS server.
The **dns backup** command configures the IP address of the backup DHS server.

Format

- **dns** *ip-address*
- **dns** *ip-address* **backup**
- **no dns**
- **no dns backup**

Parameters

Parameters	Description	Value
ip-address	Specifies the IP address of the DNS server or backup DNS server.	The value is in dotted decimal notation.

Default Value

By default, the IP address of the DNS server or backup DNS server is not configured.

View

DHCP Pool configuration view

Usage Guidelines

You can use this command to configure the IP address of the DNS server or backup DHS server.

Example

Set the IP address of the DNS server to 10.18.1.254.

```
switch(config-dhcp-pool-1)#dns 10.18.1.254
switch(config-dhcp-pool-1)#
```

3.3.19 gateway

Function

The **gateway** command configures the gateway IP address allocated by the DHCP address pool to the DHCP client.

Format

- **gateway** *ip-address*
- **no gateway**

Parameters

Parameters	Description	Value
ip-address	Specifies the gateway IP address.	The value is in dotted decimal notation.

Default Value

By default, the gateway IP address allocated by the DHCP address pool to the DHCP client is not configured.

View

DHCP Pool configuration view

Usage Guidelines

You can use this command to configure the IP address of the egress gateway router allocated by the DHCP address pool to the DHCP client.

Example

Set the gateway IP address allocated by DHCP global address pool 1 to the DHCP client to 10.18.2.1.

```
switch(config-dhcp-pool-1)#gateway 10.18.2.1
switch(config-dhcp-pool-1)#
```

3.3.20 ip dhcp

Function

The **ip dhcp** command configures the DHCP working mode.
The **no ip dhcp** command deletes the DHCP interface, and the interface does not work in any mode.

Format

- **ip dhcp** { **server** | **relay** }
- **no ip dhcp**

Parameters

Parameters	Description	Value
server	Indicates the server mode.	-
relay	Indicates the relay mode.	-

Default Value

The server or relay mode is specified in the VLAN configuration view. By default, VLAN interface does not work in any DHCP mode.

View

VLANIF configuration view

Usage Guidelines

When the DHCP works in server mode, upon receiving a DHCP packet from a DHCP client, the switch allocates an address in the DHCP server address pool.
When the DHCP works in relay mode, upon receiving a DHCP packet from a DHCP client, the switch forwards the packet to the DHCP server. Upon receiving a DHCP response packet from the DHCP server, the switch forwards it to the DHCP client.

Example

Set the DHCP working mode to relay.

```
switch(config-vlanif-3)#ip dhcp relay
switch(config-vlanif-3)#
```

3.3.21 lease-time

Function

The **lease-time** command configures the lease time of an IP address in the DHCP address pool.

Format

- **lease-time** { *time* | **default** | **unlimited** }

Parameters

Parameters	Description	Value
time	Specifies the valid lease time.	The value is an integer ranging from 1 to 120, in hours.
default	Specifies the Default Value least time.	The value is 24 hours.
unlimited	Specifies the unlimited least time.	The value is 0xFFFFFFFF.

Default Value

By default, the valid IP address least time is 24 hours, that is, 1 day.

View

DHCP Pool configuration view

Usage Guidelines

If a client uses a leased IP address dynamically allocated by a certain address pool, the client needs to re-apply for an IP address after the leased IP address expires. Most clients use IP addresses dynamically allocated by the address pool.
The least time can prevent over-long occupation of valid network resources.
The DHCP server can specify different least time for different address pools. However, the addresses in the same DHCP address pool have the same least time. The least time does not have a inheritance relationship.

Example

Set the least time of IP addresses in DHCP global address pool 1 to 48 hours.

```
switch(config-dhcp-pool-1)#lease-time 48
switch(config-dhcp-pool-1)#
```

3.3.22 lease-time day hour minute

Function

The **lease-time** command configures the lease time of an IP address in the DHCP address pool.

Format

- **lease-time day** *day* **hour** *hour* **minute** *minute*

Parameters

Parameters	Description	Value
day	Day	The value is an integer ranging from 0 to 999.
hour	Hour	The value is an integer ranging from 0 to 23.
minute	Second	The value is an integer ranging from 0 to 59.

Default Value

By default, the valid IP address least time is 24 hours, that is, 1 day.

View

DHCP Pool configuration view

Usage Guidelines

If a client uses a leased IP address dynamically allocated by a certain address pool, the client needs to re-apply for an IP address after the leased IP address expires. Most clients use IP addresses dynamically allocated by the address pool.
The least time can prevent over-long occupation of valid network resources.
The DHCP server can specify different least time for different address pools. However, the addresses in the same DHCP address pool have the same least time. The least time does not have a inheritance relationship.

Example

Set the least time of IP addresses in DHCP global address pool 1 to 1 hour 5 minutes 59 seconds.

```
switch(config-dhcp-pool-1)#lease-time day 1 hour 5 minute 59
switch(config-dhcp-pool-1)#
```

3.3.23 network mask

Function

The **network mask** command configures the range and mask of IP addresses in the DHCP address pool that can be dynamically allocated.
The **no network** command disables the operation.

Format

- **network range** *start-ip-address end- ip-address* **mask** *mask-address*
- **network** *ip-address* **mask** *mask-address*
- **no network**

Parameters

Parameters	Description	Value
start-ip-address	Specifies the start IP address allocated.	The value is in decimal notation.
end-ip-address	Specifies the end IP address allocated.	The value is in decimal notation.
mask-address	Specifies the mask address.	The value is in decimal notation.
ip-address	Specifies the network address.	The value is in decimal notation.

Default Value

By default, the range of IP addresses that are dynamically allocated is not configured.

View

DHCP Pool configuration view

Usage Guidelines

Only one network segment can be configured for each DHCP address pool. If IP addresses in multiple network segments are required, you need to configure multiple DHCP address pools.

Example

Set the range of IP addresses in DHCP global address pool 1 to 10.18.13.154~ 10.18.13.241 and mask to 255.255.255.0.

```
switch(config-dhcp-pool-1)#network range 10.18.13.154 10.18.13.241 mask 255.255.255.0
```

```
switch(config-dhcp-pool-1)#
```

3.3.24 no dhcp server bind all

Function

The **no dhcp server bind al**l command deletes all the entires bound with the DHCP server.

Format

- **no dhcp server bind all**

Parameters

None

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Delete all the entires bound with the DHCP server.

```
switch(config)#no dhcp server bind all
switch(config)#
```

3.3.25 no dhcp fake-server all

Function

The **no dhcp fake-server all** command deletes all recorded server information.

Format

- **no dhcp fake-server all**

Parameters

None

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to view information about DHCP servers on the network. After the fake server monitoring is enabled, the switch records the server IP address, VLAN, and port information in a received DHCP Relay packet.

Example

Delete all server information recorded on the switch.

```
switch(config)#no dhcp fake-server all
switch(config)#
```

3.3.26 no dhcp server expired

Function

The **no dhcp server expired** command deletes all the expired entires bound with the DHCP server.

Format

- **no dhcp server expired** *ip-address*
- **no dhcp server expired all**

Parameters

Parameters	Description	Value
ip-address	Specifies the IP address.	The value is in dotted decimal notation.

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Delete all the expired entires bound with the DHCP server.

```
switch(config)#no dhcp server expired all
switch(config)#
```

3.3.27 no dhcp server conflict

Function

The **no dhcp server conflict** deletes the DHCP server conflict table.

Format

- **no dhcp server conflict** *ip-address*
- **no dhcp server conflict all**

Parameters

Parameters	Description	Value
ip-address	Specifies the IP address.	The value is in dotted decimal notation.

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Delete the DHCP server conflict table.

```
switch(config)#no dhcp server conflict all
switch(config)#
```

3.3.28 no dhcp server dynamic-bind

Function

The **no dhcp server dynamic-bind** command deletes a dynamic DHCP binding entry.

Format

- **no dhcp server dynamic-bind** *ip-address*

Parameters

Parameters	Description	Value
ip-address	Specifies the IP address.	The value is in dotted decimal notation.

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Delete a dynamic DHCP binding entry.

```
switch(config)#no dhcp server dynamic-bind 1.1.1.1
switch(config)#
```

3.3.29 reset dhcp relay statistic

Function

The **reset dhcp relay statistic** command clears DHCP relay statistics.

Format

- **reset dhcp relay statistic**

Parameters

None

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to re-collect information in received packets.
After this command is successfully executed, all statistics of packets on the DHCP relay is cleared.

Example

Clear the statistics of the DHCP relay.

```
switch(config)#reset dhcp relay statistic
switch(config)#
```

3.3.30 reset dhcp server statistic

Function

The **reset dhcp server statistic** command clears DHCP server statistics.

Format

- **reset dhcp server statistic**

Parameters

None

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to re-collect information in received packets
After this command is successfully executed, all statistics of packets on the DHCP server is cleared.

Example

Clear statistics of the DHCP server.

```
switch(config)#reset dhcp server statistic
switch(config)#
```

3.3.31 show dhcp

Function

The **show dhcp** command displays DHCP server information on the switch.

Format

- **show dhcp**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, DHCP Pool configuration view

Usage Guidelines

None

Example

Display DHCP configuration Parameters and state information.

```
switch(config)#dhcp start
switch(config)#show dhcp
dhcp state : enable
dhcp server detect : disable
dhcp address-check-time(ms) : 500
dhcp server option82 : enable
dhcp lease-entry number : 0
dhcp bind-entry number : 0
dhcp forbidden-entry number : 0
dhcp user flush interval(seconds) : 1800
switch(config)#
```

3.3.32 show dhcp bind-entry

Function

The **show dhcp bind-entry** command shows DHCP user entry information.

Format

- **show dhcp bind-entry**

Parameters

None

Default Value

None

View

Common user view,privileged user view, global configuration view, VLANIF configuration view, DHCP Pool configuration view

Usage Guidelines

When a user successfully obtains an IP address from the DHCP address pool, a user entry is automatically added to the switch.
The output of this command includes the number of entries, IP address, MAC address, lease time of the IP address, and entry type.

Example

Display the DHCP user entry information.

```
switch#show dhcp bind-entry
 dhcp bind-entry number:
IpAddr   Mac   ExpireTime(seconds)   Type   HwFlag
      ------------------------------------------------
switch#
```

3.3.33 show dhcp config

Function

The **show dhcp config** command displays the DHCP configuration on the switch.

Format

- **show dhcp config**

Parameters

None

Default Value

None

View

Common user view ,privileged user view, global configuration view, VLANIF configuration view, DHCP Pool configuration view

Usage Guidelines

None

Example

Display the DHCP configuration.

```
switch#show dhcp config
!DHCP Configuration
dhcp address-check-time 30

!DHCP Pool Configuration
dhcp pool 1
 network range 10.18.10.2 10.18.10.254 mask 255.255.255.0
 dhcp server forbidden-ip 3.3.3.234 3.3.3.234
 gateway 10.18.2.1
 dns 10.18.1.254
 lease-time 48
 dhcp option60 "feisu"
interface vlan 10
```

```
 ip dhcp relay
switch#
```

3.3.34 show dhcp fake-server

Function

The **show dhcp fake-server** command shows information about servers on the network.

Format

- **show dhcp fake-server**

Parameters

None

Default Value

By default, the switch does not record any server information.

View

Common user view,privileged user view, global configuration view, VLANIF configuration view, DHCP Pool configuration view

Usage Guidelines

You can use this command to view information about servers on the network, including the IP address of the server and port that receives the BOOT-REPLY packets.

Example

Display fake server detection information.

```
switch#show dhcp fake-server
 IpAddr          Vid       Interface
1.1.1.1          3         10ge-1/01
switch#
```

3.3.35 show dhcp lease-entry

Function

The **show dhcp lease-entry** command shows lease management information of IP addresses in the address pool.

Format

- **show dhcp lease-entry**

Parameters

None

Default Value

None

View

Common user view ,privileged user view, global configuration view, VLANIF configuration view, DHCP Pool configuration view

Usage Guidelines

You can use this command to view lease management information of IP addresses in the address pool, including the IP address, subnet information, gateway, DNS, standby DNS, and least time.

Example

Display lease management information of IP addresses in the address pool.

```
switch#show dhcp lease-entry
dhcp lease-entry number:
IpAddr   Subnet   Gateway   DNS   DNSBackup   LeaseTime(seconds)
--------------------------------------------------------
switch#
```

3.3.36 show dhcp pool

Function

The **show dhcp pool** command shows configuration information of all DHCP address pools on the switch.

Format

- **show dhcp pool**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, DHCP Pool configuration view

Usage Guidelines

You can use this command to view configuration information of DHCP address pools on the switch, including the start/end IP address, mask address, gateway address, DHS address and backup address, lease time, interface bound with the address pool, and DHCP option43/option60.

Example

Display configuration information of the DHCP address pool.

```
switch(config)#show dhcp pool
pool 1 :
   dhcp pool start ip : 0.0.0.0
   dhcp pool end ip : 0.0.0.0
   dhcp pool mask : 0.0.0.0
   dhcp pool gateway address : 0.0.0.0
   dhcp pool dns address : 0.0.0.0
   dhcp pool dns backup address : 0.0.0.0
   dhcp pool lease time(hours) : 24
   dhcp option43 hex : ef
   dhcp option60 ascii : feisu
   dhcp pool entry number : 0
   dhcp pool entry used : 0

switch(config)#
```

3.3.37 show dhcp relay

Function

The **show dhcp relay** command shows the configuration of the DHCP relay server.

Format

- **show dhcp relay**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, DHCP Pool configuration view

Usage Guidelines

The DHCP relay function can transparently transmit DHCP broadcast packets across the networks, so that broadcast packets of the DHCP client or server can be transparently transmitted to the DHCP server or client on another network segment. Multiple DHCP clients on the network can use the same DHCP server, which saves costs and facilitates centralized management.
You can use this command to view the configuration of the DHCP relay server, including the enabling state of the DHCP relay, interface providing the relay function, and IP address of the DHCP server forwarded by the relay.

Example

Display the DHCP relay configuration.

```
switch#show dhcp relay
DHCP relay Configure!
 vlan 1
   dhcp relay mode: enable
   dhcp relay server-ip: 1.1.1.1
   dhcp option82: disable
   dhcp option82 action: keep
switch#
```

3.3.38 show dhcp relay statistic

Function

The **show dhcp relay statistic** command shows DHCP relay statistics.

Format

- **show dhcp relay statistic**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, DHCP Pool configuration view

Usage Guidelines

You can use this command to view DHCP relay statistics, including:
Packets received from the client.
Received DHCP DISCOVER packets, DHCP REQUEST packets, DHCP RELEASE packets, DHCP INFORM packets, and DHCP DECLINE packets.
DHCP packets, unicast packets, and broadcast packets sent to the DHCP client.

DHCP packets, DHCP OFFER packets, DHCP ACK packets, and DHCP NAK packets received from the DHCP server.
DHCP packets sent to the DHCP server.
DHCP error packets received from the DHPC server Error packets received by the DHCP relay, including the packets received from the DHCP server and DHCP client.

Example

Check the statistics of the DHCP relay.

```
switch(config)#show dhcp relay statistic
Bad Packets received : 0
packets received from clients : 0
DISCOVER received : 0
REQUEST received : 0
INFORM received : 0
DECLINE received : 0
RELEASE received : 0
packets received from servers : 0
OFFER received : 0
ACK received : 0
NAK received : 0
packets sent to servers : 0
packets sent to clients : 0
Unicast sent to clients : 0
Broadcast sent to clients : 0
switch(config)#
```

3.3.39 show dhcp relay user

Function

The **show dhcp relay user** command shows the information about the DHCP relay user entries (including dynamic and static entries).

Format

- **show dhcp relay user**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, DHCP Pool configuration view

Usage Guidelines

You can use this command to view user information configured on the DHCP relay server, including the user IP address, MAC address, VLAN, interface number, lease time, and type.

Example

```
# Display the user information of the DHCP relay.
switch(config)#show dhcp relay user
Total Entry(s) : 1
IP              MAC              Vid       Interface LeaseTime(seconds)  Type    ArpFlag
1.1.100.2   0010:9400:0002   unknown unknown    0                    static        no
switch(config)#
```

3.3.40 show dhcp server

Function

The **show dhcp server** command shows configuration information of the DHCP server.

Format

- **show dhcp server**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, DHCP Pool configuration view

Usage Guidelines

You can use this command to view DHCP server information, including the interface with DHCP server mode enabled.

Example

Display configuration information of the DHCP server.

```
switch#show dhcp server
DHCP server Configure!
    100gigaethnet 1/0/2
```

```
    dhcp server mode: enable
  100gigaethnet 1/0/5
    dhcp server mode: enable
switch#
```

3.3.41 show dhcp server conflict

Function

The **show dhcp server conflict** command shows address conflict statistics of the DHCP server.

Format

- **show dhcp server conflict**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, DHCP Pool configuration view

Usage Guidelines

You can use this command to view address conflict statistics of the DHCP server, including the involved address and conflict time.

Example

Display address conflict statistics of the DHCP server.

```
switch#show dhcp server conflict
Total Conflict Number : 1
 Vpn-Instance                IP              Time
 public                      10.1.1.1        2000-01-01 04:09:19
switch#
```

3.3.42 show dhcp server expired

Function

The **show dhcp server expired** command shows expired bound entries on the DHCP server.

Format

- **show dhcp server expired**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, DHCP Pool configuration view

Usage Guidelines

After an entry bound with a DHCP client is expired, the switch adds the entry to the expired entry table instead of immediately deleting the entry. If the DHCP client applies for an address again, the previously used address is allocated preferentially.

Example

Display expiration information of the DHCP server.

```
switch(config)#show dhcp server expired
switch(config)#
```

3.3.43 show dhcp server statistic

Function

The **show dhcp server statistic** command shows DHCP server statistics.

Format

- **show dhcp server statistic**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, DHCP Pool configuration view

Usage Guidelines

You can use this command to view DHCP server statistics, including:
Statistics of the DHCP server.
Number of messages sent by the DHCP client to the DHCP server.
Statistics of various types of DHCP packets sent by the DHCP client to the DHCP server.
Number of messages sent by the DHCP server to the DHCP client.

Statistics of various types of DHCP packets sent by the DHCP server to the DHCP client.
Number of unrecognized packets.

Example

Display statistics of the DHCP server.

```
switch(config)#show dhcp server statistic
Pool number : 1
Auto-bind IP address number : 0
Manual-bind IP address number : 0
Boot Request received: 0
DISCOVER received : 0
REQUEST received : 0
DECLINE received : 0
RELEASE received : 0
Boot Reply send: 0
OFFER send : 0
ACK send : 0
NAK send : 0
switch(config)#
```

3.3.44 show dhcp vlan config

Function

The **show dhcp vlan config** command shows the DHCP configuration of a specific VLAN interface

Format

- **show dhcp vlan** *vlan-id* **config**

Parameters

Parameters	Description	Value
vlan-id	Specifies the VLAN ID associated with the DHCP.	The value is an integer ranging from 1 to 4094.

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, DHCP Pool configuration view

Usage Guidelines

None

Example

Display the DHCP configuration of the VLAN interface.

```
switch(config)#show dhcp vlan 1 config
switch(config)#
```

3.4 DHCP Client Configuration Command

3.4.1 ip address dhcp {enable|disable}

Function

ip address dhcp {enable|disable} command is used to enable or disable DHCP Client to obtain IP addresses automatically.

Format

- **ip address dhcp** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	enable DHCP Client to obtain IP addresses automatically.	-
disable	disable DHCP Client to obtain IP addresses automatically.	-

Default Value

Disabled

View

VLANIF Configuration View

Usage Guidelines

When enabling DHCP Client, DHCP server or DHCP relay cannot be enabled. The three are mutual exclusion on interface.

Example

Enable the DHCP Client to obtain IP addresses automatically.

```
switch(config-vlanif-3)#ip address dhcp enable
switch(config-vlanif-3)#
```

3.4.2 ip address dhcp renew

Function

The **ip address dhcp renew** command is used to refresh the IP address obtained of DHCP Client.

Format

- **ip address dhcp renew**

Parameters

None

Default Value

None

View

VLANIF Configuration View

Usage Guidelines

Before using this command, please first use command of ip address dhcp {enable|disable}.

Example

Refresh the IP address obtained of DHCP Client.

```
switch(config-vlanif-3)#ip address dhcp renew
switch(config-vlanif-3)#
```

3.4.3 ip address dhcp release

Function

The **ip address dhcp release** command is used to release the IP address obtained by the DHCP Client.

Format

- **ip address dhcp release**

Parameters

None

Default Value

None

View

VLANIF Configuration View

Usage Guidelines

Before using this command, please first use command of ip address dhcp {enable|disable}.

Example

Release the IP address obtained by the DHCP Client.

```
switch(config-vlanif-3)#ip address dhcp release
switch(config-vlanif-3)#
```

3.4.4 dhcp client auto-config mode

Function

The **dhcp client auto-config mode** command is used to choose or cancel auto-config mode including HW mode, user defined mode and default mode.
The **no dhcp client auto-config** command is used to cancel the auto-config mode.

Format

- **dhcp client auto-config mode** { **compatible** | **user-define** | **default** }
- **no dhcp client auto-config**

Parameters

Parameters	Description	Value
compatible	HW mode	-
user-define	user defined mode	-
default	feisu network mode	-

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Choose the auto-config mode as the default mode.

```
switch(config)#dhcp client auto-config mode default
switch(config)#
```

3.4.5 dhcp client ftp-name option

Function

dhcp client ftp-name option command is used to configure ftp-name option and sub-option information.

Format

- **dhcp client ftp-name option** *option value*
- **dhcp client ftp-name option** *option value* **sub-option** *sub-option value*

Parameters

Parameters	Description	Value
option value	option value	integer, 125-254
sub-option value	sub-option value	integer, 0-254

Default Value

None

View

Global Configuration View

Usage Guidelines

None

Example

Set the ftp-name value to 125.

```
switch(config)#dhcp client ftp-name option 125
switch(config)#
```

3.4.6 dhcp client ftp-password option

Function

dhcp client ftp-password option command is used to configure ftp-password option and sub-option information.

Format

```
dhcp client ftp-password option option-value
dhcp client ftp-password option option-value sub-option sub-option-value
```

Parameters

Parameters	Description	Value
option-value	otpion value	integer, 125-254
sub-option-value	sub-option value	integer, 0-254

Default Value

None

View

Global Configuration View

Usage Guidelines

None

Example

Set the ftp-password to 125.

```
switch(config)#dhcp client ftp-password option 125
switch(config)#
```

3.4.7 dhcp client ftp-server-ip option

Function

dhcp client ftp-server-ip option command is used to configure ftp-server-ip option and sub-option information.

Format

- **dhcp client ftp-server-ip option** *option-value*
- **dhcp client ftp-server-ip option** *option-value* **sub-option** *sub-option-value*

Parameters

Parameters	Description	Value
option-value	option value	integer, 125-254
sub-option-value	sub-option value	integer, 0-254

Default Value

None

View

Global Configuration View

Usage Guidelines

None

Example

Set the ftp-server-ip to 125.

```
switch(config)#dhcp client ftp-server-ip option 125
switch(config)#
```

3.4.8 dhcp client image-file option

Function

dhcp client image-file option command is used to configure image-file option and sub-option information.

Format

- **dhcp client image-file option** *option-value*
- **dhcp client image-file option** *option-value* **sub-option** *sub-option-value*

Parameters

Parameters	Description	Value
option-value	option value	integer, 125-254
sub-option-value	sub-option value	integer, 0-254

Default Value

None

View

Global Configuration View

Usage Guidelines

None

Example

Set the image-file value to 125.

```
switch(config)#dhcp client image-file option 125
switch(config)#
```

3.4.9 dhcp client image-list option

Function

dhcp client image-list option command is used to configure imagelist-file option and sub-option information.

Format

- **dhcp client image-list option** *option-value*
- **dhcp client image-list option** *option-value* **sub-option** *sub-option-value*

Parameters

Parameters	Description	Value
option-value	option value	integer, 125-254
sub-option-value	sub-option value	integer, 0-254

Default Value

None

View

Global Configuration View

Usage Guidelines

None

Example

Set the image-list value to 125.

```
switch(config)#dhcp client image-list option 125
switch(config)#
```

3.4.10 dhcp client reboot-time option

Function

dhcp client reboot-time option command is used to configure reboot-time option and sub-option information.

Format

- **dhcp client reboot-time option** *option-value*
- **dhcp client reboot-time option** *option-value* **sub-option** *sub-option-value*

Parameters

Parameters	Description	Value
option-value	option value	integer, 125-254
sub-option-value	sub-option value	integer, 0-254

Default Value

None

View

Global Configuration View

Usage Guidelines

None

Example

Set the reboot-time value to 125.

```
switch(config)#dhcp client reboot-time option 125
switch(config)#
```

3.4.11dhcp client auth-message option

Function

dhcp client auth-message option command is used to configure auth-message option and sub-option information.

Format

- **dhcp client auth-message option** *option-value*
- **dhcp client auth-message option** *option-value* **sub-option** *sub-option-value*

Parameters

Parameters	Description	Value
option value	option value	integer, 125-254
sub-option value	sub-option value	integer, 0-254

Default Value

None

View

Global Configuration View

Usage Guidelines

None

Example

Set the auth-message value to 125.

```
switch(config)#dhcp client auth-message option 125
switch(config)#
```

3.4.12 reset dhcp client statistic

Function

reset dhcp client statistic command is used to clear the TX/RX packet statistics information of VLAN interface.

Format

- **reset dhcp client statistic**

Parameters

None

Default Value

None

View

VLANIF Configuration View

Usage Guidelines

None

Example

Clear the TX/RX packet statistics of the VLAN3 interface.

```
switch(config-vlanif-3)#reset dhcp client statistic
switch(config-vlanif-3)#
```

3.4.13 show dhcp client

Function

show dhcp client command is used to display DHCP Client state information of all or single VLAN interface.

Format

- **show dhcp client**
- **show dhcp client vlan** *vlan-id*

Parameters

Parameters	Description	Value
vlan-id	VLAN ID of interface	integer, 1-4094

Default Value

None

View

Common User View, Privilege User View, Global Configuration View, VLANIF Configuration View, DHCP Configuration View

Usage Guidelines

None

Example

Display the DHCP Client state.

```
switch(config)#show dhcp client
Dhcp client information:
Version:DHCPCLIENT_VB3.00.05.00
switch(config)#
```

3.4.14 show dhcp client auto-config vlan

Function

show dhcp client auto-config vlan command is used to display all the configuration of auto-config in a VLAN interface.

Format

- **show dhcp client auto-config vlan** *vlan-id*

Parameters

Parameters	Description	Value
vlan-id	VLAN ID of interface	integer, 1-4094

Default Value

None

View

Common User View, Privilege User View, Global Configuration View, VLANIF Configuration View, DHCP Pool Configuration View

Usage Guidelines

None

Example

Display all the configuration of auto-config in a VLAN interface.

```
switch(config)#show dhcp client atuo-config vlan 1
  Auto-config mode:user-define
  ..........................................................................
  Name                    Option     Sub-option    Information
  config file             67         0             D:¥config.txt
  tftp server-name        66         0
```

```
  tftp server-ip          150          0              10.18.11.187
  ftp-name                141          0               feisu
  ftp-password            142          0               feisu
  ftp server-ip           143          2              10.11.12.34
  image-file              145          5               D:¥linux¥vxworks
  reboot-time             146          6               17
  auth-message            148          8               imagelist.txt
  image-list              147          7              smartinstall
switch(config-vlanif-3)#
```

3.4.15 show dhcp client statistic

Function

show dhcp client statistic command is used to display DHCP Client TX/RX packet statistic information of all or single VLAN interface.

Format

- **show dhcp client statistic**
- **show dhcp client statistic vlan** *vlan-id*

Parameters

Parameters	Description	Value
vlan-id	VLAN ID of interface	integer, 1-4094

Default Value

None

View

Common User View, Privilege User View, Global Configuration View, VLANIF Configuration View, DHCP Configuration View

Usage Guidelines

None

Example

Display the Tx / Rx packet statistics of the DHCP client of the VLAN3 interface

```
switch#show dhcp client statistic
Dhcp client statistic :
Interface number:vlan-3
    Packet total        Out number: 5
    Arp                   Out number: 3
    Discover             Out number: 1
```

```
    Request              Out number: 1
    Decline              Out number: 0
    Release              Out number: 0
    Inform               Out number: 0
    Error dhcp           Out number: 0
    Error Arp            Out number: 0
    Packet total         In  number: 2
    Offer                In  number: 1
    Ack                  In  number: 1
    Nak                  In  number: 0
    Arp                  In  number: 0
    Error dhcp           In  number: 0
    Error Arp            In  number: 0
switch#
```

3.5 IPv6 Address Configuration Commands

3.5.1 flush ipv6 neighbor dynamic

Function

The **flush ipv6 neighbor dynamic** command flushes all dynamic entries in the IPv6 neighbor table.

Format

- **flush ipv6 neighbor dynamic**

Parameters

None

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to flush all dynamic entries in the IPv6 neighbor table.

Example

Flush all dynamic entries in the IPv6 neighbor table.

```
switch(config)#flush ipv6 neighbor dynamic
switch(config)#
```

3.5.2 flush ipv6 neighbor static

Function

The **flush ipv6 neighbor static** command flushes all static entries in the IPv6 neighbor table.

Format

- **flush ipv6 neighbor static**

Parameters

None

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to flush all static entries in the IPv6 neighbor table.

Example

Flush all static entries in the IPv6 neighbor table.

```
switch(config)#flush ipv6 neighbor static
switch(config)#
```

3.5.3 flush ipv6 neighbor all

Function

The **flush ipv6 neighbor all** command flushes all entries in the IPv6 neighbor table.

Format

- **flush ipv6 neighbor all**

Parameters

None

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to flush all entries in the IPv6 neighbor table.

Example

Flush all entries in the IPv6 neighbor table.

```
switch(config)#flush ipv6 neighbor all
switch(config)#
```

3.5.4 ipv6 {enable|disable}

Function

The **ipv6 {enable|disable}** command enables or disables the IPv6 function.

Format

- **ipv6 { enable | disable }**

Parameters

None

Default Value

disable

View

VLANIF configuration view, Tunnel interface configuration view, and Loopback interface configuration view

Usage Guidelines

None

Example

Enable the IPv6 function on the interface.

```
switch(config-vlanif-3)#ipv6 enable
switch(config-vlanif-3)#
```

3.5.5 ipv6 address

Function

The **ipv6 address** command configures primary and secondary IPv6 addresses for VLAN interface.
The **no ipv6 address** command deletes specified or all IPv6 addresses of a VLAN interface.

Format

- **ipv6 address** *ipv6-address/mask-length*
- **ipv6 address** *ipv6-address/mask-length* **sub**

- **no ipv6 address** i*pv6-address*
- **no ipv6 address**

Parameters

Parameters	Description	Value
ipv6-address	Specifies the IPv6 address of a VLANIF interface.	A 128-bit IPv6 address is divided into 8 groups, with 16 bits in each group. Each group is expressed by four hexadecimal digits (0-9 and A-F), and two groups are separated with a colon (:). Each X represents a group of hexadecimal digits.
mask- length	Specifies the mask length of an IPv6 address.	The value is an integer in the range from 1 to 128.

Default Value

None

View

VLANIF configuration view, Tunnel interface configuration view, and Loopback interface configuration view

Usage Guidelines

An interface can have only one primary address but can have multiple secondary addresses. Different VLAN interfaces cannot be configured with the same IPv6 address.
If an interface is not a VLAN interface, determine its working mode before configuring IPv6 addresses for it. If it works in bridge mode, the IPv6 address is not allowed.

Example

Set the primary IPv6 address to 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A and subnet mask length to 2.

```
switch(config- vlanif -3)#ipv6 address 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A/2
switch(config- vlanif -3)#
```

3.5.6 ipv6 address eui-64

Function

The **ipv6 address eui-64** command configures the global unicast address in EUI-64 format.
The **no ipv6 address eui-64** command deletes a specified global unicast address in EUI-64 format.

Format

- **ipv6 address** *ipv6-address/mask-length* **eui-64**
- **ipv6 address** *ipv6-address/mask-length* **eui-64 sub**
- **no ipv6 address** *ipv6-address* **eui-64**

Parameters

Parameters	Description	Value
ipv6-address	Specifies the IPv6 address of an interface.	A 128-bit IPv6 address is divided into 8 groups, with 16 bits in each group. Each group is expressed by four hexadecimal digits (0-9 and A-F), and two groups are separated with a colon (:). Each X represents a group of hexadecimal digits.
mask- length	Specifies the mask length of the IPv6 address.	The value is an integer in the range from 0 to 64.

Default Value

None

View

VLANIF configuration view, Tunnel interface configuration view, and Loopback interface configuration view

Usage Guidelines

None

Example

Configure the EUI-64 address of interface VLAN10.

```
switch(config- vlanif -10)#ipv6 enable
switch(config- vlanif -10)#ipv6 address 2000::1/64 eui-64
switch(config- vlanif -10)#
```

3.5.7 ipv6 address link-local

Function

The **ipv6 address link-local** command configures a local IPv6 address for a link.

Format

- **ipv6 address** *ipv6-address* **link-local**
- **no ipv6 address link-local**

Parameters

Parameters	Description	Value
ipv6-address	Specifies a local IPv6 address for a link.	A 128-bit IPv6 address is divided into 8 groups, with 16 bits in each group. Each group is expressed by four hexadecimal digits (0-9 and A-F), and two groups are

Parameters	Description	Value
		separated with a colon (:). Each X represents a group of hexadecimal digits.

Default Value

None

View

VLANIF configuration view

Usage Guidelines

Before configuring a link-local IPv6 address, you must enable the IPv6 function.
Before deleting the link-local IPv6 address, you must set the mode of generating a local address to manual, and the prefix of the local address must match FE80::/10.

Example

Set a local IPv6 address for a link to fe80::204:6717:3c90:ffff.

```
switch(config- vlanif -2)# no ipv6 address auto link-local
switch(config- vlanif -2)# ipv6 address fe80::204:6717:3c90:ffff link-local
```

3.5.8 ipv6 address auto link-local

Function

The **ipv6 address auto link-local** command enables automatic generation of a link-local IPv6 address for a VLAN interface.
The **no ipv6 address auto link-local** command deletes the automatically generated link-local IPv6 address of a VLAN interface.

Format

- **ipv6 address auto link-local**
- **no ipv6 address auto link-local**

Parameters

None

Default Value

By default, the MAC address of the switch is used to generate a link-local address.

View

VLANIF configuration view

Usage Guidelines

None

Example

Configure the automatically generated link-local address.

```
switch(config- vlanif -3)#ipv6 address auto link-local
switch(config- vlanif -3)#
```

3.5.9 ipv6 description

Function

The **ipv6 description** command describes an IPv6 address.
The **no ipv6 description** command deletes the description.

Format

- **ipv6 description** *STRING*
- **no ipv6 description**

Parameters

Parameters	Description	Value
STRING	Describes the IPv6 address.	The value is a character string. The directory name is case sensitive and cannot contain any of the following characters: space, tilde (~), asterisk (*), slash (/), back slash (¥), colon (:), and apostrophe (').

Default Value

None

View

VLANIF configuration view

Usage Guidelines

None

Example

Describe the IPv6 address configuration and set the content to test.

```
switch(config- vlanif -100)#ipv6 description test
switch(config- vlanif -100)#
```

3.5.10 ipv6 neighbor

Function

The **ipv6 neighbor** command creates a static neighbor entry in the neighbor discovery cache.
The **no ipv6 neighbor** command deletes a static neighbor entry from the neighbor discovery cache.

Format

- **ipv6 neighbor** *ipv6-address mac-address* { **igaethernet** | **xgigaethernet** } *terface-number*
- **ipv6 neighbor** *ipv6-address mac-address* **eth-trunk** *trunk-number*
- **no ipv6 neighbor** *ipv6-address*

Parameters

Parameters	Description	Value
ipv6-address	Specifies a destination IPv6 address.	A 128-bit IPv6 address is divided into 8 groups, with 16 bits in each group. Each group is expressed by four hexadecimal digits (0-9 and A-F), and two groups are separated with a colon (:). Each X represents a group of hexadecimal digits.
mac-address	Specifies a destination MAC address.	The value is in the AA:BB:CC:DD:EE:FF format, where each of the letters A to F represents a hexadecimal digit.
interface-number	Specifies an Ethernet port number.	The value is an integer in the range of 1-1/0-2/1-52.
gigaethernet	Specifies a Gigabit Ethernet interface.	-
xgigaethernet	Specifies a 10Gigabit Ethernet interface.	-
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.

Default Value

None

View

VLANIF configuration view

Usage Guidelines

None

Example

Create an IPv6 neighbor entry, in which the connected interface is 100gigaethernet1/0/1, interface IP address is 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A, and MAC address is 00:05:68:00:00:01.

```
switch(config- vlanif -3)#ipv6 neighbor 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A 00:05:68:00:00:01 100gigaethernet 1/0/1
switch(config- vlanif -3)#
```

3.5.11ipv6 mtu

Function

The **ipv6 mtu** command configures the MTU size of an IPv6 interface.

Format

- **ipv6 mtu** { *mtu-value* | **default** }

Parameters

Parameters	Description	Value
mtu-value	Specifies the MTU size.	The value is an integer ranging from 1280 to 9216, in the form of bytes.
default	Specifies the default.	The length of the value is 1280 bytes.

Default Value

The default MTU value is 1280 bytes.

View

VLANIF configuration view

Usage Guidelines

None

Example

Set the MTU of an IPv6 interface to 1400.

```
switch(config- vlanif -3)#ipv6 mtu 1400
switch(config- vlanif -3)#
```

3.5.12 ipv6 nd lifetime

Function

The **ipv6 nd lifetime** command sets the life cycle of IPv6 neighbor discovery.

Format

- **ipv6 nd lifetime** *lifetime*

Parameters

Parameters	Description	Value
lifetime	Specifies the life cycle of IPv6 neighbor discovery.	The value is an integer ranging from 30 to 86400, in seconds.

Default Value

1200s

View

Global configuration view

Usage Guidelines

None

Example

Set the life cycle of IPv6 neighbor discovery to 1140 seconds.

```
switch(config)#ipv6 nd lifetime 1440
switch(config)#
```

3.5.13 ipv6 prefix-list

Function

The**ipv6 prefix-list** command configures the IPv6 prefix list entry.
The **no ipv6 prefix-list** command cancels the configuration.

Format

- **ipv6 prefix-list** *LISTNAME* { **deny** | **permit** } *ipv6-address/mask-length*
- **ipv6 prefix-list** *LISTNAME* { **deny** | **permit** } *ipv6-address/mask-length* { **greater-equal** | **less-equal** } *prefix-length*
- **ipv6 prefix-list** *LISTNAME* { **deny** | **permit** } *ipv6-address/mask-length* **greater-equal** *prefix-length* **less-equal** *prefix-length*
- **ipv6 prefix-list** *LISTNAME* **index** *index-number* { **deny** | **permit** } *ipv6-address/mask-length*
- **ipv6 prefix-list** *LISTNAME* **index** *index-number* { **deny** | **permit** } *ipv6-address/mask-length* { **greater-equal** | **less-equal** } *prefix-length*
- **ipv6 prefix-list** *LISTNAME* **index** *index-number* { **deny** | **permit** } *ipv6-address/mask-length* **greater-equal** *prefix-length* **less-equal** *prefix-length*
- **no ipv6 prefix-list** *LISTNAME*
- **no ipv6 prefix-list** *LISTNAME* **index** *index-number*

Parameters

Parameters	Description	Value
LISTNAME	Specifies the name of a prefix list.	-
deny|permit	Specifies the action of allowing or rejecting a packet with the IP address in the list.	-
ipv6-address	Specifies an IPv6 address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of an IPv6	The value is an integer in the range from 0

Parameters	Description	Value
	address.	to 128.
greater-equal|less-equal	Specifies an action taken when the length of a prefix is no longer than or no shorter than the length of the IPv6 address prefix.	-
prefix-length	Specifies the prefix length.	The value is an integer in the range from 0 to 32.
index	Specifies the index.	-
index-number	Specifies the index number.	The value is an integer in the range from 1 to 65535.

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Configure the action of permitting entry 123 with IPv6 address 10:10::10:10, mask length 24, and prefix of no shorter than 20.

```
switch(config)#ipv6 prefix-list 123 permit 1000::/64 greater-equal 20
switch(config)#
```

3.5.14 ipv6 unicast-forwarding {enable|disable}

Function

The **ipv6 unicast-forwarding {enable|disable}** command enables or disables the IPv6 unicast forwarding.

Format

- **ipv6 unicast-forwarding** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the IPv6 unicast forwarding.	-
disable	Disables the IPv6 unicast forwarding.	-

Default Value

Enable

View

Global configuration view

Usage Guidelines

None

Example

Disable the IPv6 unicast forwarding.

```
switch(config)#ipv6 unicast-forwarding disable
switch(config)#
```

3.5.15 show ipv6 neighbor

Function

The **show ipv6 neighbor** command displays IPv6 neighbor information.

Format

- **show ipv6 neighbor**

Parameters

None

Default Value

None

View

Privileged user view, global configuration view, common user view, VLANIF configuration view

Usage Guidelines

None

Example

Display the IPv6 neighbor information.

```
switch(config)#show ipv6 neighbor
IPv6Addr                L2Addr              Interface   State       Last-update Type
switch(config)#
```

3.5.16 show ipv6 interface

Function

The **show ip6 interface** command displays IPv6 interface information.

Format

- **show ipv6 interface**

Parameters

None

Default Value

None

View

Privileged user view, global configuration view, common user view, VLANIF configuration view

Usage Guidelines

None

Example

Display IPv6 interface information.

```
switch#show ipv6 interface
  The total number of ipv6 address: 1

  Interface        State(a/o)  Addr/Len     Status          Role          Type
  loopback-0       up/up         ::1/128    preferred       primary         auto

switch#
```

3.5.17 show ipv6 interface loopback

Function

The **show ipv6 interface loopback** command displays the IPv6 loopback interface information.

Format

show ipv6 interface loopback *loopback-number*

Parameters

Parameters	Description	Value
loopback-number	Specifies a loopback interface	The value is an integer in the range

Parameters	Description	Value
	number.	from 1 to 1024.

Default Value

None

View

Common user view, privileged user view, global configuration view, and VLANIF configuration view

Usage Guidelines

None

Example

Set the IPv6 address of the interface loopback 1 to 2001::1/64 and display the IPv6 loopback interface information.

```
switch(config-loopback-1)#ipv6 address 2001::1/64
switch(config)#show ipv6 interface loopback 1
 Interface loopback-1
          Physical Address: 00:50:01:FC:C1:CB     description: N/A
          Admin state:up    Oper state:up
          IPv6 Addr :fe80::250:1ff:fefc:c1cb/64     Role:linklocal    Type:auto
          IPv6 Addr :2001::1/64     Role:primary    Type:static
          NDP RA MTU :131072     Vpn instance    :N/A
switch(config)#
```

3.5.18 show ipv6 interface vlan

Function

The **show ipv6 interface vlan** command displays the IPv6 VLAN interface information.

Format

- **show ipv6 interface vlan** *vlan-id*

Parameters

Parameters	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

Privileged user view, global configuration view, common user view, VLANIF configuration view

Usage Guidelines

None

Example

Display IPv6 interface information.

```
switch#show ipv6 interface vlan 2
Interface vlan-2
        Physical Address: 00:00:00:00:DE:AD     Admin state:UP,Oper state:down
        IPv6 Addr :fe80::204:6717:3c90:ffff/64     Role:linklocal    Type:unknown
        NDP RA MTU :1500
switch#
```

3.5.19 show ipv6 statistic interface vlan

Function

The **show ipv6 statistic interface vlan** command displays IPv6 statistics on a specific VLAN.

Format

- **show ipv6 statistic interface vlan** *vlan-id*

Parameters

Parameters	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.

Default Value

None

View

Privileged user view, global configuration view, common user view

Usage Guidelines

None

Example

Display IPv6 statistics on VLAN 2.

```
switch(config)#show ipv6 statistic interface vlan 2
IPv6 Protocol:
```

```
Interface:vlan-2

 Sent packets:
        Total                 : 8
        Forwarded             : 0          Discarded             : 0
        Fragments             : 0          Fragmented            : 0
        Fragments failed      : 0          Multicast             : 4
        Raw packets           : 4

 Received packets:
        Total                 : 0          Header error          : 0
        Too big               : 0          Routing failed        : 0
        Address error         : 0          Protocol error        : 0
        Truncated             : 0          Discarded             : 0
        Delivers              : 0          Multicast             : 0
        Reassembly            : 0          Reassembled           : 0
        Reassemble failed     : 0
```

3.5.20 show ipv6 statistic

Function

The **show ipv6 statistic** command displays IPv6 statistics.

Format

- **show ipv6 statistic**

Parameters

None

Default Value

None

View

Privileged user view, global configuration view, common user view, VLANIF configuration view

Usage Guidelines

None

Example

Display IPv6 statistics on VLAN 2.

```
switch(config)#show ipv6 statistic
IPv6 Protocol:
```

```
Interface:vlan-2
    Sent packets:
        Total                 : 18
        Forwarded             : 0          Discarded             : 0
        Fragments             : 0          Fragmented            : 0
        Fragments failed      : 0          Multicast             : 6
        Raw packets           : 12
    Received packets:
        Total                 : 6          Header error          : 0
        Too big               : 0          Routing failed        : 0
        Address error         : 0          Protocol error        : 0
        Truncated             : 0          Discarded             : 0
        Delivers              : 6          Multicast             : 1
        Reassembly            : 0          Reassembled           : 0
        Reassemble failed     : 0
```

3.5.21 show ipv6 route summary

Function

The **show ipv6 route summary** command shows the routing information summarized by IPv6.

Format

- **show ipv6 route summary**

Parameters

None

Default Value

None

View

Privileged user view, global configuration view, common user view, VLANIF configuration view

Usage Guidelines

None

Example

Display the routing information summarized by IPv6.

```
switch(config)#show ipv6 route summary
 Bad routing redirect: 0
 Dynamically created route: 0
 New gateway due to redirects: 0
```

```
Destination found unreachable: 1916
Use of a wildcard route: 0
Software route: 3
Hardware route: 6
```

3.5.22 show ipv6 neighbor

Function

The **show ipv6 neighbor** command displays IPv6 neighbor information.

Format

- **show ipv6 neighbor**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, and VLANIF configuration view

Usage Guidelines

None

Example

Display IPv6 neighbor information.

```
switch(config)#show ipv6 neighbor
IPv6Addr                L2Addr          Interface   State       Last-update Type
switch(config)#
```

3.5.23 show ipv6 neighbor summary

Function

The **show ipv6 neighbor summary** command displays the routing information of neighbors summarized by IPv6.

Format

- **show ipv6 neighbor summary**

Parameters

None

Default Value

None

View

Privileged user view, global configuration view, common user view, VLANIF configuration view

Usage Guidelines

None

Example

Display the routing information of neighbors summarized by IPv6.

```
switch(config)#show ipv6 neighbor summary
Software route: 0
Hardware route: 0
```

3.5.24 show {ipv6|ip} prefix-list

Function

The **show {ipv6|ip} prefix-list** command shows entry information in the IPv6 or IPv4 address prefix list.

Format

- **show** { **ipv6** | **ip** } **prefix-list**
- **show** { **ipv6** | **ip** } **prefix-list** *list-name*

Parameters

Parameters	Description	Value
list-name	Specifies the name of an entry in the IPv6 or IPv4 address prefix list.	The value is a character string.

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Show the information about the fs entry in the IPv4 address prefix list.

```
switch(config)#show ip prefix-list fs
```

```
switch(config)#
```

4. Routing Commands

4.1 Overview

This chapter introduces the static routing configuration commands of the N-series switch.

4.2 Static Route Configuration Commands

4.2.1 ip route-static

Function

The **ip route-static** command creates a static IPv4 route.
The **no ip route-static** command deletes a static IPv4 route.
The **no ip route-static all** command deletes all static IPv4 routes.

Format

- **ip route-static** *ip-address mask-address nexthop-address*
- **ip route-static** *ip-address mask-address nexthop-address* **preference** *preference-value*
- **ip route-static preference** { *value* | **default** }
- **no ip route-static** *ip-address mask-address*
- **no ip route-static** *ip-address mask-address nexthop-address*
- **no ip route-static all**

Parameters

Parameters	Description	Value
ip-address	Specifies the destination IP address.	The value is in the dotted decimal format, for example, A.B.C.D, where A-D are decimal numbers in the range from 0 to 255.
mask-address	Specifies the destination IP address and subnet mask.	The value is in the dotted decimal format, for example, A.B.C.D, where A-D are decimal numbers in the range from 0 to 255.
nexthop-address	Specifies the IP address of the next hop of routing.	The value is in the dotted decimal format, for example, A.B.C.D, where A-D are decimal numbers in the range from 0 to 255.
preference-value	Specifies the preference value of the route.	The value is an integer in the range from 1 to 255.
value	Specifies the preference of the route.	The value is an integer in the range from 1 to 255.

Default Value

By default, no static routing entry is configured for the system.

View

Global configuration view

Usage Guidelines

None

Example

Configure an IPv4 route with destination IP address 220.181.111.88 and next-hop address 220.181.111.89. Delete the preceding static route and all static routes.

```
switch(config)#ip route-static 220.181.111.88 255.255.255.255 220.181.111.89
switch(config)#

switch(config)#no ip route-static 220.181.111.88 255.255.255.255 220.181.111.89
switch(config)#

switch(config)#no ip route-static all
switch(config)#
```

4.2.2 ipv6 route-static

Function

The **ipv6 route-static** command creates a static IPv6 route.
The **no ipv6 route-static** command deletes a static IPv6 route.
The **no ipv6 route-static all** command deletes all static IPv6 routes.

Format

- **ipv6 route-static** *ipv6-address mask-length ipv6-nexthop-address*
- **ipv6 route-static** *ipv6-address mask-length ipv6-nexthop-address* **preference** *preference*
- **ipv6 route-static** *ipv6-address mask-length ipv6-nexthop-address* **track bfd** *track-bfd*
- **no ipv6 route-static** *ipv6-address mask-length*
- **no ipv6 route-static track bfd all**
- **no ipv6 route-static** *ipv6-address mask-length ipv6-nexthop-address*
- **no ipv6 route-static** *ipv6-address mask-length ipv6-nexthop-address* **track bfd**
- **no ipv6 route-static all**

Parameters

Parameters	Description	Value
ipv6-address	Specifies the destination IPv6 address.	A 128-bit IPv6 address is divided into 8 groups, with 16 bits in each group. Each group is expressed by four hexadecimal digits (0-9 and A-F), and two groups are separated with a colon (:). Each X represents a group of hexadecimal digits.
mask-length	Specifies the mask length of the destination IPv6 address.	The value is an integer in the range from 0 to 128.
ipv6-nexthop-address	Specifies the next hop IPv6 address of the route.	A 128-bit IPv6 address is divided into 8 groups, with 16 bits in each group. Each group is expressed by four hexadecimal

Parameters	Description	Value
		digits (0-9 and A-F), and two groups are separated with a colon (:). Each X represents a group of hexadecimal digits.
preference	Specifies the routing priority.	The value is an integer in the range from 1 to 255.
track-bfd	Enables the static route and binds it with the static BFD session to implement quick fault detection.	The value is an integer in the range from 1 to 500.

Default Value

By default, no static IPv6 routes exist in the system.

View

Global configuration view

Usage Guidelines

The following IPv6 routes cannot be deleted:

- Filtered host routes with the mask length of 128 bits
- Multicast routes with the first byte being 0xff
- Routes with the destination addresses being the link-local addresses
- Local routes of which the protocol type is local

Example

Set an IPv6 route to 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A and the next hop address to 21DA:D3:0:2F3B:2AA:FF:FE20:8C6A.

```
switch(config)#ipv6 route-static 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A 24 21DA:D3:0:2F3B:2AA:FF:FE20:8C6A
switch(config)#
```

4.2.3 ipv6 route-static interface vlan link-local

Function

The **ipv6 route-static interface vlan link-local** command configures a static IPv6 route and specifies a link-local address as the next-next-hop address of the outgoing interface.

Format

- **ipv6 route-static** *ipv6-address mask-length* **interface vlan** *vlan-id* **link-local** *link-local-address*

Parameters

Parameters	Description	Value

Parameters	Description	Value
ipv6-address	Specifies the destination IPv6 address.	A 128-bit IPv6 address is divided into 8 groups, with 16 bits in each group. Each group is expressed by four hexadecimal digits (0-9 and A-F), and two groups are separated with a colon (:). Each X represents a group of hexadecimal digits.
mask- length	Specifies the mask length of the destination IP address.	The value is an integer in the range from 0 to 128.
vlan-id	Specifies a VLAN ID.	The value is an integer in the range from 1 to 4094.
link-local-address	Specifies a link-local IPv6 address.	A 128-bit IPv6 address is divided into 8 groups, with 16 bits in each group. Each group is expressed by four hexadecimal digits (0-9 and A-F), and two groups are separated with a colon (:). Each X represents a group of hexadecimal digits.

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Set a static route whose destination address is 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A, next hop address is the link-local address FE80::9CC5:FF28 and outgoing interface is VLAN 10.

```
switch(config)#ipv6 route-static 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A 24 interface vlan 10 link-local FE80::9CC5:FF28
switch(config)#
```

4.2.4 show ip config

Function

The **show ip config** command displays the IP address configuration.

Format

- **show ip config**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Show the IP address configuration.

```
switch#show ip config
!ip address configuration
 outband ip address 10.18.12.120/24
!
!Ip Configuration
 ip arp aging-time 600
switch#
```

4.2.5 show ip route

Function

The **show ip route** command displays route information.

Format

- **show ip route**
- **show ip route** *ip-address*
- **show ip route** *ip-address mask-address next-hop-address*

Parameters

Parameters	Description	Value
ip-address	Specifies the destination IP address.	The value is in the dotted decimal format, for example, A.B.C.D, where A-D are decimal numbers in the range from 0 to 255.
mask-address	Specifies the mask address.	The value is in dotted decimal notation.

Parameters	Description	Value
next-hop-address	Specifies the next hop address.	The value is in dotted decimal notation.

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

The destination IP address suffixed to this command specifies the information about a specified route.

Example

View local routing information.

```
switch#show ip route
  Routing Tables: Public
  Total: 2          Static: 0          Down: 0
  Destination       Gateway            Preference/Metric    Interface        Proto   Mpls
  127.0.0.0/8       127.0.0.1          0/0                  loopback-0       local   no
  192.168.11.0/24   192.168.11.11      0/0                  vlan-1           local   no

switch#
```

4.2.6 show ipv6 route

Function

The **show ipv6 route** command displays IPv6 route information.

Format

- **show ipv6 route**
- **show ipv6 route** *ipv6-address*

Parameters

Parameters	Description	Value
ipv6-address	Specifies an IPv6 address.	A 128-bit IPv6 address is divided into 8 groups, with 16 bits in each group. Each group is expressed by four hexadecimal digits (0-9 and A-F), and two groups are separated with a colon (:). Each X represents a group of hexadecimal digits.

Default Value

None

View

Common user view, privileged user view, global configuration view, and VLANIF configuration view

Usage Guidelines

None

Example

Display the IPv6 routing information.

```
switch(config)#show ipv6 route
Dest/Prefixlen                Nexthop                 Interface               Protocol Cost
switch(config)#
```

4.2.7 show {ip|ipv6} route statistic

Function

The **show {ip|ipv6} route statistic** command shows the comprehensive route statistics of the IPv4/IPv6 routing table.

Format

- **show ipv6 route statistic**
- **show ip route statistic**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, and VLANIF configuration view

Usage Guidelines

The output of this command includes:

- Proto: Routing protocol
- total routes: Total number of routes in the current routing table
- active routes: Number of active routes in the routing table
- added routes: Number of routes added to the routing table (active and inactive)
- deleted routes: Number of routes with deletion tags in the routing table

Example

Display route statistics in the IPv4 routing table.

```
switch#show ip route statistic
  Proto      total      active     added      deleted
             routes     routes     routes     routes
  DIRECT     1          1          2          1
  STATIC     0          0          0          0
  RIP        0          0          0          0
  OSPF       0          0          0          0
  IS-IS      0          0          0          0
  BGP        0          0          0          0
  Other      0          0          0          0
switch#
```

4.2.8 show {ip|ipv6}route summary

Function

The **show {ip|ipv6} route summary** command shows the summarized routing information.

Format

- **show** { **ip** | **ipv6** } **route summary**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, and VLANIF configuration view

Usage Guidelines

The output of this command includes:

- Total route entry
- Bad routing redirect
- Dynamically created route
- New gateway due to redirects
- Destination found unreachable
- Use of a wildcard route

Example

Show the summarized routing information.

```
switch#show ip route summary
 Software route                :1
 Hardware route                :1
 Software ILM                  :0
 Hardware ILM                  :0
switch#
```

4.3 RIP Configuration Command

4.3.1 debug rip

Function

The **debug rip** command can be used to turn on rip protocol debugging.
The **no debug rip** command can be used to turn off rip protocol debugging.

Format

- **debug rip { pkt-in |pkt-out |rx |tx |error |sync-rx |sync-tx |sync-detail |socket-msg |socket-msg-detail |rt-trace |all }**
- **no debug rip { pkt-in |pkt-out |rx |tx |error |sync-rx |sync-tx |sync-detail |socket-msg |socket-msg-detail |rt-trace |all }**

Parameters

None

Default Value

Disable

View

Common user view, privileged user view, global configuration view.

Usage Guidelines

This command can be used to view the RIP protocol flow path and the status of receiving and dispatching，also can be used to maintain and debug the RIP function.

Example

#Turn on all RIP debugging functions.

```
switch#debug rip all
switch#
```

4.3.2 host-route

Function

The **host-route** command can be used to configure RIP routers to support receiving host routes.
The **no host-route** command can be used to disable the RIP router to receive the host route.

Format

- **host-route**
- **no host-route**

Parameters

None

Default Value

Enable

View

Route rip configuration view.

Usage Guidelines

In some special cases, the router receives a large number of host routes from the same network segment.These routes have little effect on routing addressing but consume a lot of resources.At this point, configurable RIP prohibits receiving host routing.

Example

#Start the RIP routing process.

```
switch(config-rip-1)#host-route
switch(config-rip-1)#
```

4.3.3 ip rip filter-policy export| import route-policy

Function

IP rip filter-policy export| import routing-policy command is used to configure the inbound or outbound filtering policies based on the interface. Only the filtered routes can be added to the rip routing database.

Format

- **ip rip filter-policy {export | import} route-policy** *NAME*
- **ip rip** *rip-process* **filter-policy {export | import} route-policy** *NAME*
- **no ip rip filter-policy {export | import} route-policy**
- **no ip rip** *rip-process* **filter-policy {export | import} route-policy**

Parameters

Parameters	Description	Value
export	Outgoing direction filtering strategy.	-
import	Incoming direction filtering strategy	-
NAME	Routing policy name	Character String，not more than 20 bytes.
rip-process	rip process number	The value is an integer in the range of 1-16.

Default Value

Empty string that no routing policy is referenced.

View

Vlanif Interface configuration view.

Usage Guidelines

This command can be used to filter routing entries in updated packets received by the rip specified interface. Only routes through filtering strategy can be added to the rip routing database with the routing policy name specified by NAME.
Interface-based inbound or outbound filtering can only configure one routing policy, and if the configuration is repeated, the new policy overrides the previous one.

Example

Configure switch1, an interface - based outgoing filtering policy.

```
switch(config-vlanif-2)#ip rip filter-policy export route-policy switch1
switch(config-vlanif-2)#
```

4.3.4 ip rip authentication

Function

IP rip authentication command is used to configure the authentication method and parameters of RIPv2.
no ip rip authentication command can be used to cancel RIPv2 authentication.

Format

- **ip rip authentication text** *text-key*
- **ip rip** *rip-process* **authentication text** *text-key*
- **ip rip authentication md5** *key-id md5-key*
- **ip rip** *rip-process* **authentication md5** *key-id md5-key*
- **no ip rip authentication**
- **no ip rip** *rip-process* **authentication**

Parameters

Parameters	Description	Value
text	Set plaintext authentication	-
text-key	Plaintext validation keywords	The value is a string in the range of 1-16,no spaces supported and case sensitivity.
md5	Set MD5 authentication	-
key-id	MD5 authentication id	The value is an integer in the range of 1-255
md5-key	MD5 authentication keywords	The value is a string in the range of 1-16,no spaces supported and case sensitivity.
rip-process	Rip process number	The value is an integer in the range of 1-16.

Default Value

By default, rip authentication is not configured.

View

Vlanif Interface configuration view.

Usage Guidelines

In the absence of authentication, the device may receive some illegal routing updates that may originate from some malicious attacker, or an exception to routing information due to incorrect configuration by an administrator. To avoid these problems and improve network security, users can configure rip authentication using this command.
The RIP V1 version does not support authentication.

Example

The identifier configured for MD5 cipher text authentication is 1,the cipher text verification keyword is test.

```
switch(config-vlanif-2)#ip rip authentication md5 1 test
switch(config-vlanif-2)#
```

4.3.5 ip rip default-metric

Function

ip rip default-metric command is used to configure routing metrics for RIP.
ip rip *rip-process* **default-metric** command is used to configure routing metrics for the RIP instance.

Format

- **ip rip default-metric** { *cost* | **default** }
- **ip rip** *rip-process* **default-metric** { *cost* | **default** }

Parameters

Parameters	Description	Value

cost	Configure the default routing cost	The value is an integer in the range of 1-16,the interface does not send the default route when configured to 0.
default	The RIP default route metric is 0,indicates that the interface does not send the default route.	The value is 0.
rip-process	Rip process number	The value is an integer in the range of 1-16.

Default Value

By default, the value is 0.

View

Vlanif Interface configuration view.

Usage Guidelines

When this parameter is configured to a non-zero value, the RIP interface notifies the default route entry regardless of whether a default route exists in the RIP routing database.When configured to zero, the interface does not announce the default route unless a default route entry already exists in the RIP routing database.

Example

Configure RIP with a default metric of 12.

```
switch(config-vlanif-2)#ip rip default-metric 12
switch(config-vlanif-2)#
```

4.3.6 ip rip metric-in/out

Function

IP rip metric-in/out command is used to configure the metric offsets of routing messages that are sent or received.

Format

- **ip rip metric-in** {*metric-in number* | default)
- **ip rip** *rip-process* **metric-in** {*metric-in numbe* | default)
- **ip rip metric-out** {*metric-in number*| default)
- **ip rip** *rip-process* **metric-out** {*metric-in number*| default)

Parameters

Parameters	Description	Value
metric-in number	An offset to a routing item metric in a received message.	The value is an integer in the range of 1-15.
metric-out number	An offset to a routing item metric in a sending message.	The value is an integer in the range of 1-15.

Parameters	Description	Value
metric-in number	An offset to a routing item metric in a received message.	The value is an integer in the range of 1-15.
rip-process	Rip process number.	The value is an integer in the range of 1-16.

Default Value

By default, metric-in is 0 and metric-out is 1.

View

Vlanif Interface configuration view.

Usage Guidelines

Additional metrics are added to the original RIP routing metrics, including sending additional metrics and receiving additional metrics.Sending additional metrics does not change the routing metrics in the routing table, and they are added to the routing only when the interface sends RIP routing information.

Example

Configure RIP with a metric-in of 12.

```
switch(config-vlanif-2)#ip rip metric-in 12
switch(config-vlanif-2)#
```

4.3.7 ip rip passive-interface

Function

ip rip passive-interface command is used to configure the RIP interface in silent mode.
no ip rip passive-interface command is used to cancel the RIP interface in silent mode

Format

- **ip rip** *rip-process* **passive-interface**
- **no ip rip** *rip-process* **passive-interface**

Parameters

Parameters	Description	Value
rip-process	Rip process number	The value is an integer in the range of 1-16.

Default Value

none

View

VLANIF Interface configuration view.

Usage Guidelines

Use this command to configure the RIP interface in silent mode.The RIP interface of the router receives only RIP packets and does not send RIP packets.

Example

Configure RIP silence mode.

```
switch(config-vlanif-3)#ip rip passive-interface
switch(config-vlanif-3)#
```

4.3.8 ip rip receive-version

Function

ip rip receive-version command is used to configure the version of RIP that the interface allows to receive.
ip rip *rip-process* **receive-version** command is used to configure the version of the RIP packets that the RIP instance interface allows to receive.

Format

- **ip rip receive-version** { **v1** | **v2** | **v1v2** | **no-receive** }
- **ip rip** *rip-process* **receive-version** { **v1** | **v2** | **v1v2** | **no-receive** }

Parameters

Parameters	Description	Value
v1	Receive RIP-1 packets	-
v2	Receive RIP-2 packets	-
v1v2	Receive RIP-1 and RIP-2 packets	-
no-receive	RIP packets are not accepted	-
rip-process	Rip process number	The value is an integer in the range of 1-16.

Default Value

By default, the interface is allowed to receive v1v2 packets.

View

VLANIF Interface configuration view.

Usage Guidelines

RIP must be enabled before configuration, and the IP address,RIP routing of the interface must have been enabled.

Example

#Configure the VLANIF 3 interface to allow RIP-1 packets to be received

```
switch(config-vlanif-3)#ip rip receive-version v1
switch(config-vlanif-3)#
```

4.3.9 ip rip send-version

Function

ip rip send-version command sets the version that RIP packets are sent.
ip rip *rip-process* **send-version** command sets the version on a specified RIP process that RIP packets are sent.

Format

- **ip rip send-version** { **no-send** | **v1** | **v1-compatible** | **v2** }
- **ip rip** *rip-process* **send-version** { **no-send** | **v1** | **v1-compatible** | **v2** }

Parameters

Parameters	Description	Value
rip-process	Specifies a RIP process.	The value is an integer ranging from 1 to 16.
no-send	No RIP packets are sent.	-
v1	Only sends RIP-1packets	-
v1-compatible	RIP-V2 packets are sent in broadcast mode.	-
v2	RIP-V2 packets are sent in multicast mode.	-

Default Value

By default, the interface can sends both RIP-1 and RIP-2 packets.

View

VLANIF interface view

Usage Guidelines

Before starting with the configuration, the RIP process must be started and enable RIP for the interface on the specified network segement.

Example

#Sets vlanif 3 to send RIP-1 version.

```
switch(config-vlanif-3)#ip rip send-version v1
switch(config-vlanif-3)#
```

4.3.10 split-horizon {enable|disable}

Function

split-horizon enable enables split horizon.
split-horizon disable disables split horizon and uses poison-reverse.

Format

- **split-horizon enable**
- **split-horizon disable**

Parameters

Parameters	Description	Value
enable	enable split horizon function	-
disable	diables split horizon function	-

Default Value

By default, split horizon is enabled.

View

router rip configuration view

Usage Guidelines

Generally, it is necessary to enable split-horizon to avoid routing loops between neighboring devices. Only in some special cases, disables split horizon and running **poison-reverse enable** command to enable poison reverse.

Example

#Enable split horzon

```
switch(config-rip)#split-horizon enable
switch(config-rip)#
```

4.3.11ip rip timer basic

Function

ip rip timer basic command sets the value of RIP timers.

Format

- **ip rip timer basic** *{update | Expire | garbage }*

Parameters

Parameters	Description	Value
update	Specifies the interval for sending update packets.	The value is an integer ranging from10 to 3600, in seconds.
expire	Specifies the time for aging routes.	The value is an integer ranging from40 to 14400, in seconds.
garbage	Specifies the time for deleting a invalid route from routing table.	The value is an integer ranging from40 to 14400, in seconds.

Default Value

By default, the interval for sending update packets is 30s, the time for aging routes is 180s, the time for deleting a route from the routing table is 120s.

View

router rip configuration view

Usage Guidelines

This command can configure the value of RIP timers. Expire timer no less than 4 times update timer, garbage timer no less than 4 times update timer, and the value of aging time must be less than the value of garbage. By default, the interval for sending update packets is 30s, the time for aging routes is 180s, the time for deleting a route from the routing table is 120s.The value of update timer is ranging from 10 to 3600, because the rip packets are sent by broadcast or multicast, if the interval of sending update packets is too small to aggravate network loads, so the value of update time is recommended not to set below 30, in seconds.

Example

#Set the interval for sending update packets to 10s, if the route cannot receive the update packets within 80s, the corresponding route becomes invalid and enters invalid state, garbage timer is set to 200s.

```
switch(config-rip)#ip rip timer basic 10 80 200
switch(config-rip)#
```

4.3.12 default-route originate {enable|disable}

Function

default-route originate enable command is set to enable originating a default route to neighbors.
default-route originate disable command is set to disable originating a default route to neighbors.

Format

- **default-route originate enable**
- **default-route originate disable**

Parameters

Parameters	Description	Value

Parameters	Description	Value
enable	enable originating a default-route.	-
disable	disable originating a default-route.	-

Default Value

By default, enable originating a default-route.

View

router rip configuration view

Usage Guidelines

In general, the device do not support originating a default-route when running RIP, you should run this command to enable originating a default-route.

Example

Enable originating a default-route.

```
switch(config-rip)#default-route originate enable
switch(config-rip)#
```

4.3.13 poison-reverse {enable|disable}

Function

poison-reverse enable enables poison reverse.
poison-reverse disable disables poison reverse.

Format

- **poison-reverse enable**
- **poison-reverse disable**

Parameters

Parameters	Description	Value
enable	enable poison-reverse function	-
disable	diables poison-reverse function	-

Default Value

By default, poison-reverse is disabled.

View

Rip router configuration view

Usage Guidelines

- After poison reverse is enabled, RIP sets the cost of the routes learned from a specified interface to 16 (indicating unreachable), and then sends the routes to neighbors through the same interface.
- When both split horizon and poison reverse are configured, only poison reverse takes effect.

Example

#Enable poison reverse function.

```
switch(config-rip)# poison-reverse enable
switch(config-rip)#
```

4.3.14 network

Function

network command enables RIP for the interface on the specified network segment.
no network command disables RIP for the interface on the specified network segment.

Format

- **network** *network-address*
- **no network** *network-address*

Parameters

Parameters	Description	Value
network-address	Specifies the network address on which RIP is enabled. It must be the address of the natural network segment.	The value is in dotted decimal notation.

Default Value

By default, RIP is disabled for all the interfaces.

View

router rip configuration view

Usage Guidelines

RIP only run on the interface for specified network segment which RIP process is enable. RIP does not receive and send route, nor forward it on the interface for specified network segmet which RIP process is disable,

Example

Enable RIP routes for the interface on 10.18.13.12 network segment.

```
switch(config-vlanif-100)#ip address 10.18.13.12/24
switch(config-vlanif-100)#quit
switch(config)#router rip
```

```
switch(config-rip)#network 10.18.13.12
switch(config-rip)#
```

4.3.15 router rip

Function

router rip command starts the specified RIP process and enters this RIP process view.
no router rip command stops the specified RIP process.

Format

- **router rip**
- **router rip** *process-id*
- **no router rip** [*process-id*]

Parameters

Parameters	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer that ranges from 1 to 16. The default value is 1.

Default Value

By default, no RIP process is started.

View

Global Configuration View

Usage Guidelines

Before configuring each global RIP parameter, you need to start RIP. All the RIP configuration parameters will be invalid if the specified RIP process is stopped.

Example

Starts the specified RIP process.

```
switch(config)#route rip
switch(config-rip)#
```

4.3.16 validate-source-address

Function

validate-source-address command is set to check the validity source IP address in RIP update packets.
no router rip command disables check on source IP addresses in RIP Update packets

Format

- **validate-source-address**
- **no validate-source-address**

Parameters

None

Default Value

None

View

route rip configuration view

Usage Guidelines

After the **validate-source-address** command is executed, RIP checks whether the IP addresses of interfaces that send and receive the Update packets are on the same network segment. If not, the device does not process the packets.

Example

Enable source address check.

```
switch(config-rip)#validate-source-address
switch(config-rip)#
```

4.3.17 show ip rip

Function

show ip rip displays the configuration of a RIP process.

Format

- **show ip rip** *rip-process*

Parameters

Parameters	Description	Value
rip-process	Specified a RIP process.	The value is an integer that ranges from 1 to16.

Default value

None

View

All views

Usage Guidelines

None

Example

Display the configuration information of a specified RIP process.

```
switch(config)#show ip rip 2
Rip instance 2
        Status                                  :enable
        VPN name                                :--
        Splithorizen                            :enable
        Redistribute static                     :disable
        Redistribute ospf                       :disable
        Redistribute connect                    :disable
        Redistribute bgp                        :disable
        Redistribute isis                       :disable
        Default cost                            :0
        Update time                             :30
        Expired time                            :180
        Garbage time                            :300
        Default-route                           :disable
        Check-zero                              :enable
        validate-source-address                 :enable
        host-route                              :enable
        Network                                 :30.1.1.1
        Network                                 :40.1.1.1

switch(config)#
```

4.3.18 show ip rip resource

Function

show ip rip resource command displays all the resource configuration information of RIP interfaces.

Format

- **show ip rip resource**

Parameters

None

Default value

None

View

All views.

Usage Guidelines

You can use this command to display all the resource configuration information of RIP interfaces, including recent number of routes and so on.

Example

Display all the resource configuration information of RIP interfaces.

```
switch(config)#show ip rip resource
 rip route current num: 0
 rip route max num: 262144
 rip route interface current num: 0
 rip route interface max num: 577
 rip route peer current num: 0
 rip route peer max num: 1731
 ip rip timer basic 10 80 200
 redistribute static
 no redistribute connect
 no redistribute ospf
 no redistribute bgp
 ip rip splithorizen enable
switch(config)#
```

4.3.19 show ip rip config

Function

show ip rip config command displays the configuration information of a RIP process.

Format

- **show ip rip config**

Parameters

None

Default Value

None

View

All views

Usage Guidelines

When the global configuration is set to the default value, nothing can be displayed running this command.

Example

#Display the RIP configuration information.

```
switch#show ip rip config
!
!Rip Configuration
 router rip 1 vpn-instance vpn1
 network 10.1.1.1
 network 20.1.1.1
 router rip 2
 network 30.1.1.1
 network 40.1.1.1
switch#
```

4.3.20 show ip rip database

Function

show ip rip database command displays all the active routes in the RIP database. These routes are sent in RIP Update packets.

Format

- **show ip rip database**
- **show ip rip** *rip-process* **database**
- **show ip rip database** *ip-address Dst-Mask*
- **show ip rip** *rip-process* **database** *ip-address Dst-Mask*

Parameters

Parameters	Description	Value
ip-address	Specifies the destination IP address of a route.	The value is in dotted decimal notation.
Dst-Mask	Specifies the IP address mask address	The value is in dotted decimal notation.
rip-process	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 16.

Default Value

None

View

All views

Usage Guidelines

You can run this command to display the routes that can be sent in RIP packets. Including destination IP address segement, mask, next-hop, metric, aging time, state and protocol of a route.
The routing table of parameters are shown in the following table.

Parameters	Description	Value
gateway	Next-hop address	The value is in dotted decimal notation
Metric	Distance metric	The value is in decimal system
age	Ageing-time	The value is a decimal system in seconds
state	Routing state	Active or Down
proto	Protocol type	The value is a string

Example

#Display all RIP route information that can be sent.

```
switch#show ip rip database
  rip route count = 2
destination          netmask              gateway              metric age     state    proto
3.3.3.0              255.255.255.0        3.3.3.1              0         0         ACTIVE rip
4.4.4.0              255.255.255.0        4.4.4.1              0         0         ACTIVE rip
switch#
```

#Display RIP 2 route information that can be sent.

```
switch# show ip rip 2 database
rip route count = 2
Instance destination    netmask    gateway    metric age    state    proto    tag
2         30.1.1.0    255.255.255.0    30.1.1.1     0       0    DOWN    rip     0
2       40.1.1.0 255.255.255.0       40.1.1.1     0     0     DOWN      rip     0
switch#
```

4.3.21 show ip rip interface

Function

show ip rip interface command displays information about RIP interfaces.

Format

- **show ip rip** *rip-process* **interface**
- **show ip rip interface**

Parameters

Parameters	Description	Value
rip-process	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 16

Default Value

None

View

All views

Usage Guidelines

This command displays the configuration and running status of RIP, which facilitate fault location and configuration verification.

Example

#Display information about RIP on interfaces.

```
switch(config)#show ip rip interface
Interface                    :vlan-20
 Interface status            :Down
 Interface passive mode      :False
 Interface adress            :20.1.1.1
 Interface netmask           :255.0.0.0
 Authtication Type           :no authtication
 Send Version                :rip version 1 compatible
 Receive Version             :rip version 1 or version 2
 Interface defaulte metric :0
 Interface metric-in :0
 Interface metric-out :1
```

#Display information about RIP process 2 on interfaces.

```
switch(config)# show ip rip 2 interface
Instance                     :2
Interface                    :vlan-30
Interface status             :Down
Interface passive mode       :False
Interface adress             :30.1.1.1
Interface netmask            :255.255.255.0
Authtication Type            :no authtication
```

```
Send Version                    :rip version 1 compatible
Receive Version                 :rip version 1 or version 2
Interface defaulte metric       :0
Interface metric-in             :0
Interface metric-out            :1
Instance                        :2
Interface                       :vlan-40
Interface status                :Down
Interface passive mode          :False
Interface adress                :40.1.1.1
Interface netmask               :255.255.255.0
Authtication Type               :no authtication
Send Version                    :rip version 1 compatible
Receive Version                 :rip version 1 or version 2
Interface defaulte metric       :0
Interface metric-in             :0
Interface metric-out            :1
```

4.3.22 show ip rip neighbor

Function

show ip rip neighbor command displays information about RIP neighbors.

Format

- **show ip rip neighbor**
- **show ip rip** *rip-instance* **neighbor**

Parameters

Parameters	Description	Value
rip-instance	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 16.

Default Value

None

View

All views

Usage Guidelines

None

Example

Display information about the neighbor in RIP process 1.

```
switch#show ip rip neighbor
switch#
```

4.4 OSPFv2 Configuration Commands

4.4.1 filter route-policy

Function

The **filter route-policy** command configures the routing protocol filter policy. Only filtered routes can be used to generate routes in the routing table.
The **no filter router-policy** command cancels the routing protocol filter policy.

Format

- **filter route-policy** *route-policy-name*
- **no filter route-policy** *route-policy-name*

Parameters

Parameters	Description	Value
route-policy-nam	Specifies a routing policy name, configured in the routing policy.	The value string characters.

Default Value

By default, the value is a string of blank characters, indicating that no routing policy is referenced.

View

OSPFv2 route configuration view

Usage Guidelines

Only routing information in compliance with certain conditions can be used to generate routes in the routing table.
You can use this command to set filter conditions for routing information. Only filtered information can be used to generate routes in the routing table.
Before running this command, you must run the route-policy command to create a routing policy.

Example

Configure filter policy feisu1 for the routing protocol.

```
switch(config-ospf-1)#filter route-policy feisu1
switch(config-ospf-1)#
```

4.4.2 valid-ttl-hops

Function

The **valid-ttl-hops** command sets the valid TTL value of OSPF.

Format

valid-ttl-hops { *hops-number* | **default** }

Parameters

Parameters	Description	Value
hops-number	Specifies the number of hops.	The value is an integer ranging from 1 to 255.
default	Specifies the default number of hops.	0

Default Value

The default is 0.

View

OSPFv2 route configuration view

Usage Guidelines

If the TTL is not configured, OSPF does not detect the TTL by default. When the TTL is configured and the TTL of a received packet is smaller than 255-hops number+1, the switch discards the packet.

Example

Set the valid TTL of OSPF to 200.

```
switch(config-ospf-1)#valid-ttl-hops 200
switch(config-ospf-1)#
```

4.4.3 area range

Function

The **area range** command configures the aggregation route entry in an area.
The **no area range** command deletes the aggregation route entry configured for an area.

Format

- **area** *area-id* **range** *dst-address dst-mask* { **advertise** | **no-advertise** }
- **no area** *area-id* **range** *dst-address dst-mask*

Parameters

Parameters	Description	Value

Parameters	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
dst-address	Specifies an aggregation address.	The value is in dotted decimal notation.
dst-mask	Specifies an aggregation mask.	The value is in dotted decimal notation.
advertise	Indicates that the switch receives aggregation entries.	-
no-advertise	Indicates that the switch rejects aggregation entries.	-

Default Value

By default, the OSPF area does not include any aggregation entry

View

OSPFv2 route configuration view

Usage Guidelines

Before running this command, you must create an area.
You can use this command to configure an aggregation route entry for an area. You can use the no area range command to delete an aggregation entry configured for an area.
When the ABR calculates the route for area A, it advertises the internal routes of area A to other areas, and generates a Summary LSA for each area. If the internal route scale is large, the number of Summary LSA entries is large. You can configure aggregation entry for area A to control the number of Summary LSAs.
After the aggregation entry is configured, routes matching the aggregation entry in area A will not be included in the Summary LSAs of other areas. According to different advertise attributes of the aggregation entries, the following situations may exist:
1.The advertise operation is specified for the aggregation entry, and the Summary LSA is generated for the aggregation entry.
2.The not-advertise operation is specified for the aggregation entry, and the Summary LSA is not generated for the aggregation entry.

Warning: This command can only be used for an existing area.

Example

The following command enables area 0 to include only Summary LSA of 1.1.0.0/16.

```
switch(config-ospf-1)#network 1.1.0.0 255.255.255.0 area 0
```

```
switch(config-ospf-1)#
switch(config-ospf-1)#area 0 range 1.1.0.0 255.255.0.0 advertise
```

Th# The following command enables area 1 not include any Summary LSA of 1.1.0.0/16.

```
switch(config-ospf-1)#network 1.1.0.0 255.255.255.0 area 1
switch(config-ospf-1)#
switch(config-ospf-1)#area 0 range 1.1.0.0 255.255.0.0 no-advertise
```

4.4.4 area nssa range

Function

The **area nssa range** command configures the aggregation route entry in the NSSA area.
The **no area nssa range** command deletes the aggregation route entry configured for the NSSA area.

Format

- **area** *area-id* **nssa range** *dst-address dst-mask* { **advertise** | **no-advertise** }
- **no area** *area-id* **nssa range** *dst-address dst-mask*

Parameters

Parameters	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
dst-address	Specifies an aggregation address.	The value is in dotted decimal notation.
dst-mask	Specifies an aggregation mask.	The value is in dotted decimal notation.
advertise	Indicates that the switch receives aggregation entries.	-
no-advertise	Indicates that the switch rejects aggregation entries.	-

Default Value

None

View

OSPFv2 route configuration view

Usage Guidelines

Before running this command, you must create an area.

Example

Configure the aggregation route entry in the NSSA area 1.

```
switch(config-ospf-1)#network 2.2.2.0 255.255.255.0 area 1
switch(config-ospf-1)#area 1 nssa range 2.2.2.2 255.255.255.0 advertise
switch(config-ospf-1)#
```

4.4.5 area virtual-link

Function

The **area virtual-link** command configures an OSPF virtual link.
The **no area virtual-link** command deletes an OSPF virtual link.

Format

- **area** *area-id* **virtual-link** *neighbor-address*
- **area** *area-id* **virtual-link** *neighbor-address* **hello-interval** { *hello-interval-time* | **default** }
- **area** *area-id* **virtual-link** *neighbor-address* **transmit-delay** { *transmit- interval-time* | **default** }
- **area** *area-id* **virtual-link** *neighbor-address* **retransmit-interval** { *retransmit-interval-time* | **default** }
- **area** *area-id* **virtual-link** *neighbor-address* **dead-interval** } { *dead-interval-time* | **default** }
- **area** *area-id* **virtual-link** *neighbor-address* **authentication simple-password** *key*
- **area** *area-id* **virtual-link** *neighbor-address* **authentication simple-password** { **cipher** | **plain** } *text-key*
- **area** *area-id* **virtual-link** *neighbor-address* **authentication md5** *key-id key*
- **area** *area-id* **virtual-link** *neighbor-address* **authentication md5** *key-id* **key** { **cipher** | **plain** } *key*
- **no area** *area-id* **virtual-link** *neighbor-address*
- **no area** *area-id* **virtual-link** *neighbor-address* **authentication**

Parameters

Parameters	Description	Value
area-id	Specifies the area ID of a transit area.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
neighbor-address	Specifies the router ID of a virtual neighbor.	The value is in dotted decimal notation.
dead-interval-time	Specifies the dead interval of the virtual neighbor.	dead-intervalIt is an integer ranging from 0 to 2147483647 (unit: s).
transmit-interval-time	Specifies the delay for transmitting a link status notification.	It is an integer ranging from 0 to 3600 (unit: s).
hello-interval-time	Specifies the interval for calling a virtual neighbor.	It is an integer ranging from 1 to 65535 (unit: s).

Parameters	Description	Value
retransmit-interval	Specifies the interval for retransmitting a link status notification.	It is an integer ranging from 0 to 3600 (unit: s).
key-id	Specifies the discriminator of MD5 cipher-text authentication.	It is an integer ranging from 1 to 255.
key	Specifies the keyword for authentication.	The value is a character string.

Default Value

By default, virtual links are established based on the default Parameters.

View

OSPFv2 route configuration view

Usage Guidelines

In OSPF, the backbone area summarizes topology information of areas to form an inter-area route. Therefore, all inter-area communication traffic passes through the backbone area, while non-backbone areas cannot directly exchange data packets. On the OSPF network, all non-backbone areas should be connected to the backbone area. If not due to line reasons or design reasons or the backbone area is discontinuous, certain routes cannot be calculated. Therefore, virtual links can be configured to address such problem.
Virtual link configuration must comply with the following rules:
The virtual link must be configured on the boundary switch between two areas.
An area through which the virtual link passes is known as a transit area. The transit area must have all route selection information, so that the switch can identify a physical route destined for the backbone area to transmit virtual link information.
The transit area cannot be a stub area.

Example

Configure the virtual link for area 1.

```
switch(config-ospf-1)#area 1 virtual-link 1.1.1.1
switch(config-ospf-1)#
```

4.4.6 area authentication

Function

The **area authentication** command configures plain-text authentication or MD5 authentication for an OSPF area.
The **no area authentication** command cancels the OSPF area authentication configuration.

Format

- **area** *area-id* **authentication simple-password** *text-key*
- **area** *area-id* **authentication simple-password** { **cipher** | **plain** } *text-key*
- **area** *area-id* **authentication md5** *key-id md5-key*

- **area** *area-id* **authentication md5** *key-id* { **cipher** | **plain** } *md5-key*
- **no area** *area-id* **authentication**

Parameters

Parameters	Description	Value
simple-password	Specifies the plain-text authentication mode.	-
text-key	Specifies the key word for plain-text authentication.	The value is a character string.
md5	Specifies the MD5 ciphertext authentication mode.	-
key-id	Specifies the discriminator of MD5 ciphertext authentication.	The value is an integer ranging from 1 to 255.
md5-key	Specifies the key word for ciphertext authentication.	The value is a string of 1 to 17 characters.
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.

Default Value

By default, OSPF area authentication is not configured.

View

OSPFv2 route configuration view

Usage Guidelines

You can use this command to configure MD5 authentication for an area. After configuration, all interfaces within the area use the same MD5 authentication password. You can run the no area authentication command to cancel the area authentication. Then, all interfaces within the area do not perform authentication.
Before running this command, you must create an area.

Example

Set MD5 authentication password of area 0 to aaa and KEY ID to 100.

```
switch(config)#router ospf
switch(config-ospf-1)#
switch(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
```

```
switch(config-ospf-1)#area 0 authentication md5 100 aaa
switch(config-ospf-1)#
```

4.4.7 area default-cost

Function

The **area default-cost** command configures the cost of an OSPF area.

Format

- **area** *area-id* **default-cost** { *cost* | **default** }

Parameters

Parameters	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
cost	Specifies the cost.	The value is an integer ranging from 0 to 65535.
default	Uses the default overhead value.	0

Default Value

By default, the LSA cost generated by the OSPF Stub area is 0.

View

OSPFv2 route configuration view

Usage Guidelines

The ABR in the Stub area generates default Summary LSA for the area. By default, the LSA cost is 0. You can use this command to set the cost of the SummaryLSA (for example, you need to differentiate priorities of two ABRs). You can run the no command to restore the cost to default 0.
Before running this command, you must create an area.

Example

Set the default cost of area 1 to 300.

```
switch(config)#router ospf
switch(config-ospf-1)#
switch(config-ospf-1)#network 2.2.2.0 255.255.255.0 area 1
switch(config-ospf-1)#area 1 default-cost 300
```

```
switch(config-ospf-1)#
```

4.4.8 area nssa default-cost

Function

The **area nssa default-cost** command configures the Default Value NSSA LSA cost.

Format

- **area** *area-id* **nssa default-cost** { *cost-value* | **default** }

Parameters

Parameters	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
cost-value	Specifies the cost.	The value is an integer ranging from 0 to 65535.

Default Value

None

View

OSPFv2 route configuration view

Usage Guidelines

Before running this command, you must create an area.

Example

Set the default NSSA LSA cost to 3000.

```
switch(config)#router ospf
switch(config-ospf-1)#
switch(config-ospf-1)#network 2.2.2.0 255.255.255.0 area 1
switch(config-ospf-1)#area 1 nssa default-cost 3000
switch(config-ospf-1)#
```

4.4.9 area nssa translator

Function

The **area nssa translator** command configures a specified transition router or candidate transition router for the ABR in the NSSA area.

Format

- **area** *area-id* **nssa translator** { **always** | **candidate** }

Parameters

Parameters	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
always	Specifies a transition router for the ABR in the NSSA area. Multiple ABRs in the NSSA area can be configured as thetransition router.	-
candidate	Specifies a candidate transition router for the ABR in the NSSA area. If no conversion router is designated in the current area, the conversion router is elected from all the candidate routers.	-

Deault Value

None

View

OSPFv2 route configuration view

Usage Guidelines

Before running this command, you must create an area.

Example

Specify a transition router for the ABR in the NSSA area.

```
switch(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 10000
switch(config-ospf-1)#area 10000 nssa translator always
switch(config-ospf-1)#
```

4.4.10 area nssa

Function

The **area nssa** command configures an OSPF area as an NSSA area.
The **no area nssa** command restores an NSSA area as a common area.

Format

- **area** *area-id* **nssa**
- **no area** *area-id* **nssa**

Parameters

Parameters	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.

Default Value

By default, the NSSA is disabled in OSPF areas.

View

OSPFv2 route configuration view

Usage Guidelines

The NSSA area is similar to the Stub area. The difference is that the NSSA area can send external routes but does not receive routes from the external. The router in the NSSA area generates Type7 LSA for the external route. The LSA calculates the routes based on the external route within the area. The ABR converts Type7 LSA into Type5 LSA and sends it to other areas. The ABR also generates a default Summary LSA for the NSSA area.
The NSSA area has the following limitations:
NSSA cannot be configured for the backbone area.

NSSA cannot be configured for the Stub area.
NSSA cannot be configured for the virtual link transit area.

Exampe

Set area 1 as an NSSA area.

```
switch(config)#router ospf
switch(config-ospf-1)#
switch(config-ospf-1)#network 2.2.2.0 255.255.255.0 area 1
switch(config-ospf-1)#area 1 nssa
switch(config-ospf-1)#
```

4.4.11area te

Function

The **area te** command enables or disables the OSPF TE function..

Format

- **area** *area-id* **te** { **enable** | **disable** }

Parameters

Parameters	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
enable	Enables the OSPF TE function.	-
disable	Disables the OSPF TE function.	-

Default Value

None

View

OSPFv2 route configuration view

Usage Guidelines

None.

Exaple

Enable the OSPF TE function.

```
switch(config-ospf-1)#area 2 te enable
switch(config-ospf-1)#
```

4.4.12 area stub

Function

The **area stub** command configures an OSPF area as a stub area.
The **no area stub** command restores a stub area as a common area.

Format

- **area** *area-id* **stub** [**no-summary**]
- **no area** *area-id* **stub**

Parameters

Parameters	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address.The value ranges from 0 to 4294967295.
[no-summary]	After this Parameters is configured, the ABR generates default Summary LSA only for the stub area.	-

Default Value

By default, the NSSA is disabled in OSPF areas.

View

OSPFv2 route configuration view

Usage Guidelines

You can use this command to configure an area as a stub area. The stub area does not include external routes (Type5LSA) and does not generate external routes. The stub area configuration has the following limitations:
The backbone area cannot be configured as a stub area.

If an area is a virtual link transit area, you cannot configure this area as a stub area. Otherwise, the area works abnormally.
After a stub area is configured, the ABR generates a default Summary LSA for the area. The generation process of other Summary LSAs remains unchanged. If the no-summary attribute is configured, the ABR clears other non- default Summary LSAs and includes only one default Summary LSA.
A Stub area can control the number of LSAs within an area. If an area has limited router memory and cannot receive a large amount of LSAs, you can configure this area as a Stub area.
A Stub area cannot be used as the virtual link transit area. All routers within a Stub area must have the same stub attributes. Otherwise, a neighbor relation cannot be established.

Example

Rstore a Stub area as a common area.

```
switch(config-ospf-1)#no area 1 stub
switch(config-ospf-1)#
```

4.4.13 area stub no-summary

Function

The **area stub no-summary** command configures an area as a Totally Stub area.

Format

- **area** *area-id* **stub no-summary**

Parameters

Parameters	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address.The value ranges from 0 to 4294967295.

Default Value

None

View

OSPFv2 route configuration view

Usage Guidelines

Before running this command, you must create an area.
The ABR in an area can stop generating other Summary LSAs for the Stub area to further compress the LSA scale. At this time, the Stub area is known as a Totally Stub area.

Example

Configure area 1.3.2.1 as a Totally Stub area.

```
switch(config-ospf-1)#area 1.3.2.1 stub no-summary
switch(config-ospf-1)#
```

4.4.14 area nssa no-summary

Function

The **area nssa no-summary** command configures an area as a Totally NSSA area.

Format

- **area** *area-id* **nssa no-summary**

Parameters

Parameters	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address.The value ranges from 0 to 4294967295.

Default Value

None

View

OSPFv2 route configuration view

Usage Guidelines

Before running this command, you must create an area.

Example

Configure area 1 as a Totally NSSA area.

```
switch(config-ospf-1)#area 1 nssa no-summary
switch(config-ospf-1)#
```

4.4.15 graceful-restart begin

Function

The **graceful-restart begin** command implements graceful restart.

Format

- **graceful-restart begin**

Parameters

None

Default Value

None

View

OSPFv2 route configuration view

Usage Guidelines

None

Example

Implement graceful restart.

```
switch(config-ospf-1)#graceful-restart begin
switch(config-ospf-1)#
```

4.4.16 graceful-restart helper

Function

The **graceful-restart helper** command enables or disables the OSPF graceful restart helper

Format

- **graceful-restart helper**
- **no graceful-restart helper**

Parameters

None

Default Value

None

View

OSPFv2 route configuration view

Usage Guidelines

None

Example

Enable the OSPF graceful restart helper.

```
switch(config-ospf-1)#graceful-restart helper
switch(config-ospf-1)#
```

4.4.17 graceful-restart

Function

The **graceful-restart** command enables the graceful restart function.
The **graceful-restart period** command specifies the period of graceful restart.
The **no graceful-restart** command disables the graceful restart function.

Format

- **graceful-restart**
- **graceful-restart period** *restart-time*
- **no graceful-restart**

Parameters

Parameters	Description	Value
restart-time	Specifies the restart time.	The value is an integer ranging from 40 to 1800, in seconds.

Default Value

None

View

OSPFv2 route configuration view

Usage Guidelines

Before configuring the graceful restart, you must manually enable opaque.

Example

Enable graceful restart.

```
switch(config-ospf-1)#graceful-restart
switch(config-ospf-1)#
```

4.4.18 ip ospf dead-interval

Function

The **ip ospf dead-interval** command configures the neighbor expiration time of an IPv4 OSPF interface.

Format

- **ip ospf dead-interval** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	Specifies the neighbor expiration time of the OSPF interface.	The value is an integer ranging from 0 to 2147483647.
default	Specifies the default neighbor expiration time of the OSPF interface.	40 seconds

Default Value

By default, the neighbor expiration time of the OSPF interface is 40s.

View

VLANIF configuration view, Loopback interface configuration view

Usage Guidelines

You can use this command to modify the default neighbor expiration time of the OSPF interface. Note that the same expiration time must be configured for both parties and the value must be larger than 3xInterval for sending Hello packets.

Example

Set the neighbor expiration time of an OSPF interface to 30s.

```
switch(config-vlanif-3)#ip ospf dead-interval 30
switch(config-vlanif-3)#
```

4.4.19 ip ospf hello-interval

Function

The **ip ospf hello-interval** command configures the interval for sending Hello packets by an IPv4 OSPF interface.

Format

- **ip ospf hello-interval** { *hello-interval* | **default** }

Parameters

Parameters	Description	Value
hello-interval	Specifies the interval for sending Hello packets an OSPF interface.	The value is an integer ranging from 1 to 65535.
default	Specifies the Default Value interval for sending Hello packets by an OSPF interface.	10 seconds

Default Value

The default is 10s.

View

VLANIF configuration view, Loopback interface configuration view

Usage Guidelines

By default, the interval for sending Hello packets by an OSPF interface is 10s. You can modify the default, but the interval configured for both parties must be the same. The interval must be smaller than neighbor expiration time/3.

Example

Set the interval for sending Hello packets by the OSPF interface to 20s.

```
switch(config-vlanif-3)#ip ospf hello-interval 20
switch(config-vlanif-3)#
```

4.4.20 ip ospf authentication

Function

The **ip ospf authentication** command configures the OSPF interface authentication mode.

Format

- **ip ospf authentication md5** *key-id* { **cipher** | **plain** } *md5-key*
- **ip ospf authentication md5** *key-id md5-key*
- **ip ospf authentication simple-password** *key-value*
- **ip ospf authentication simple-password** { **cipher** | **plain** } *key-value*
- **no ip ospf authentication**

Parameters

Parameters	Description	Value
simple-password	Configures simple password authentication for the interface.	The value is a string of 1 to 9 characters.
md5	Configures the MD5 authentication for	-

Parameters	Description	Value
	the interface.	
key-id	Specifies the discriminator of MD5 ciphertext authentication.	The value is an integer ranging from 1 to 255.
md5-key	Specifies the key word for ciphertext authentication.	The value is a string of 1 to 17 characters. The value does not support spaces and is case-sensitive.
key-value	Specifies the authentication key of a simple password.	The value is a character string.

Default Value

None

View

VLANIF configuration view, Loopback interface configuration view

Usage Guidelines

The interface authentication configuration shall prevail if the interface authentication configuration and area authentication configuration co-exist.

Example

Configure MD5 authentication for an OSPF interface.

```
switch(config-vlanif-3)#ip ospf authentication md5 100 key
switch(config-vlanif-3)#
```

Configure simple password authentication for an OSPF interface.

```
switch(config-vlanif-3)#ip ospf authentication simple-password key
switch(config-vlanif-3)#
```

4.4.21 ip ospf bfd

Function

The **ip ospf bfd** command enables or disables the BFD function of a VLAN interface.

Format

- **ip ospf bfd** { **enable** | **disable** }

Parameters

Parameters	Description	Value

Parameters	Description	Value
enable	Enables the BFD function.	-
disable	Disables the BFD function.	-

Default Value

None

View

VLANIF configuration view, Loopback interface configuration view

Usage Guidelines

After the BFD is enabled, the switch can rapidly discover the disconnection of an OSPF neighbor.

Example

Enables the BFD function.

```
switch(config-vlanif-3)#ip ospf bfd enable
switch(config-vlanif-3)#
```

4.4.22 ip ospf cost

Function

The **ip ospf cost** command configures the OSPF interface cost.

Format

- **ip ospf cost** { *cost* | **default** }

Parameters

Parameters	Description	Value
cost	Specifies the cost required for running the OSPF protocol.	The value is an integer ranging from 1 to 65535.
default	Specifies the default cost required for running the OSPF protocol.	The value is automatic setting.

Default Value

None

View

VLANIF configuration view, Loopback interface configuration view

Usage Guidelines

The OSPF interface cost is used for route selection control. For example, compared with 100 Mbit/s interface, the capacity of the 1000 Mbit/s interface is larger. Therefore, you can set a smaller cost for the 1000 Mbit/s interface, so that it can be selected preferentially. Generally, interfaces on adjacent routers should be configured with the same cost.

Example

Set OSPF interface cost to 20000.

```
switch(config-vlanif-3)#ip ospf cost 20000
switch(config-vlanif-3)#
```

4.4.23 ip ospf fast-change

Function

The **ip ospf fast-change** command configures the fast neighbor establishment for an OSPF interface.

Format

- **ip ospf fast-change** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the fast neighbor establishment for an OSPF interface.	-
disable	Disables the fast neighbor establishment for an OSPF interface.	-

Default Value

None

View

VLANIF configuration view

Usage Guidelines

None

Example

Enable the fast neighbor establishment for an OSPF interface.

```
switch(config-vlanif-3)#ip ospf fast-change enable
switch(config-vlanif-3)#
```

4.4.24 ip ospf flooding-group

Function

The **ip ospf flooding-group** command configures the OSPF flooding group.

Format

- **ip ospf flooding-group** *flooding-group-number*

Parameters

Parameters	Description	Value
flooding-group-number	Non-0: If the value is not 0, interfaces within the same flooding group do not spread the LSA. If the value is 0, the configuration restores to the normal mode.	The value is an integer ranging from 0 to 64.

Default Value

The default is 0.

View

VLANIF configuration view

Usage Guidelines

None

Example

Configure OSPF flooding group 1.

```
switch(config-vlanif-3)#ip ospf flooding-group 1
switch(config-vlanif-3)#
```

4.4.25 ip ospf if-type

Function

The **ip ospf if-type** command configures the network type of an OSPF interface.

Format

- **ip ospf if-type** { **broadcast** | **p2p** }

Parameters

Parameters	Description	Value
broadcast	Changes the network type of an interface to broadcast.	-

Parameters	Description	Value
p2p	Changes the network type of an interface to point-to-point.	-

Default Value

By default, the interface type of an OSPF interface is broadcast.

View

VLANIF configuration view, Loopback interface configuration view

Usage Guidelines

The switch interfaces are Ethernet interfaces. By default, the interface type of OSPF interfaces is broadcast. The operation of broadcast interfaces is more complex than that of point-to-point interfaces. In actual situations, if a switch adopts the point-to-point connection, you need to change the interface type of the OSPF interfaces to point-to-point. Generally, it is recommended that interfaces on both parties in a neighbor relation are configured as point-to-point interfaces. Otherwise, the operation may be abnormal.

Example

Set the interface network type of an OSPF interface to p2p.

```
switch(config-vlanif-3)#ip ospf if-type p2p
switch(config-vlanif-3)#
```

4.4.26 ip ospf mtu

Function

The **ip ospf mtu** command configures the MTU size of an OSPF interface.

Format

- **ip ospf mtu** { *mtu* | **default** }

Parameters

Parameters	Description	Value
mtu	Specifies the MTU size of an OSPF interface.	The value is an integer ranging from 572 to 1500.
default	Specifies the default MTU size of an OSFP interface.	The value is 1500.

Default Value

The default is 1500.

View

VLANIF configuration view

Usage Guidelines

The default MTU of the OSPF interface is the IPMTU of the interface. If the interface does not support MTU configuration, the value is 0 by default. You can use this command to modify the MTU of the OSPF interface. Note that this command is not used to modify the MTU of an IP interface.
You must configure the same MTU value for both parties in a neighbor relation.

Example

Set the MTU value of an OSPF interface to 1000.

```
switch(config-vlanif-3)#ip ospf mtu 1000
switch(config-vlanif-3)#
```

4.4.27 ip ospf mtu-ignore {enable|disable}

Function

The **ip ospf mtu-ignore {enable|disable}** command enables or disables the MTU detection function of an interface.

Format

- **ip ospf mtu-ignore** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables MTU detection.	-
disable	Disables MTU detection.	-

Default Value

disable.

View

VLANIF configuration view, Loopback interface configuration view

Usage Guidelines

None

Example

Enables MTU ignore detection.

```
switch(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
switch(config-ospf-1)#quit
switch((config-vlanif-1)#ip ospf mtu-ignore enable
switch((config-vlanif-1)#
```

4.4.28 ip ospf passive-interface

Function

The **ip ospf passive-interface** command configures an OSPF passive interface.
The **no ip ospf passive-interface** command cancels the configuration.

Format

- **ip ospf passive-interface**
- **no ip ospf passive-interface**

Parameters

None

Default Value

None

NoneView

VLANIF configuration view and Loopback interface configuration view

Usage Guidelines

A passive interface refers to an OSPF interface that does not send or receive protocol messages and does not establish any neighbor relation. However, the interface route is included in the Router LSA for internal route propagation. The passive interface can be used on the Stub route.

Example

Configure the VLAN 3 interface as the passive interface of OSPF.

```
switch(config-vlanif-3)#ip ospf passive-interface
switch(config-vlanif-3)#
```

4.4.29 ip ospf poll-interval

Function

The **ip ospf poll-interval** command specifies the interval for sending polling Hello packets by a neighbor router on the NBMA network.

Format

- **ip ospf poll-interval** { *poll-interval-time* | **default** }

Parameters

Parameters	Description	Value
poll-interval-time	Specifies the interval for sending polling Hello packets by a neighbor router on the	The value is an integer ranging

Parameters	Description	Value
	NBMA network.	from 1 to 3600, in seconds.
default	Specifies the default.	120s

Default Value

The default is 120s.

View

VLANIF configuration view, Loopback interface configuration view

Usage Guidelines

None

Example

Set the interval for sending polling Hello packets by a neighbor router on the NBMA network to 2000s.

```
switch(config-vlanif-3)#ip ospf poll-interval 2000
switch(config-vlanif-3)#
```

4.4.30 ip ospf priority

Function

The **ip ospf priority** command configures the OSPF interface priority.

Format

- **ip ospf priority** { *priority*| **default** }

Parameters

Parameters	Description	Value
priority	Specifies the OSPF interface priority.	The value is an integer ranging from 0 to 255, in bytes/s.
default	Specifies the default OSPF interface priority.	The value is 1.

Default Value

The default is 1.

View

VLANIF configuration view and Loopback interface configuration view

Usage Guidelines

The OSPF interface priority is used for DR election. Generally, it does not need to be configured, especially in the point-to-point connection scenario, since the interface priority is basically useless. However, if you require a specific interface functioning as the DR, you can set a higher priority for the interface. Note that the DR of OSPF interfaces cannot be preempted. If a device serves as the DR, it constantly serves as the DR unless it is faulty or disabled.

Example

Set OSPF interface priority to 125.

```
switch(config-vlanif-3)#ip ospf priority 125
switch(config-vlanif-3)#
```

4.4.31 ip ospf retransmit-interval

Function

The **ip ospf retransmit-interval** command configures the retransmission interval for an OSPF interface.

Format

- **ip ospf retransmit-interval** { *retransmit-interval-time* | **default** }

Parameters

Parameters	Description	Value
retransmit-interval-time	Specifies the retransmission interval.	The value is an integer ranging from 0 to 3600, in seconds.
default	Specifies the default retransmission interval.	The value is 5s.

Default Value

The default is 5s.

View

VLANIF configuration view and Loopback interface configuration view

Usage Guidelines

OSPF packets are directly encapsulated based on IP for transmission. There is a probability of packet loss. Therefore, packet retransmission is required. The default retransmission interval is 5s. You can adjust the retransmission interval according to the network conditions.
The retransmission interval is a variable and does not need synchronization. You can configure different retransmission intervals for both parties in a neighbor relation.

Example

Set the retransmission interval of an OSPF interface to 2s.

```
switch(config-vlanif-3)#ip ospf retransmit-interval 2
switch(config-vlanif-3)#
```

4.4.32 ip ospf transmit-delay

Function

The **ip ospf transmit-delay** command configures the transmission delay of an OSPF interface.

Format

- **ip ospf transmit-delay** { *transmit-delay-time* | **default** }

Parameters

Parameters	Description	Value
transmit-delay-time	Specifies the transmission delay of an interface.	The value is an integer ranging from 0 to 3600, in seconds.
default	Specifies the default.	1

Default Value

1

View

VLANIF configuration view

Usage Guidelines

OSFP assumes that a delay is generated during message transmission. The default delay is 1s. Delay is set to better control the LSA update. For example, when an LSA with Age set to 0 is transmitted over an interface, Age should be set to the delay of the interface. However, considering the aging time of the LSA is 3600s, which is much larger than the actual transmission delay of the interface, the transmission delay is not important.
The retransmission delay is a variable and does not need synchronization. You can configure different retransmission delay values for both parties in a neighbor relation.

Example

Set the transmission delay of an OSPF interface to 2s.

```
switch(config-vlanif-3)#ip ospf transmit-delay 2
switch(config-vlanif-3)#
```

4.4.33 network area

Function

The **network area** command configures the OSPF area.
The **no network area** command deletes the OSPF area.

Format

- **network** *network-address network-mask* **area** *area-id*
- **no network** *network-address network-mask* **area** *area-id*

Parameters

Parameters	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
network-address	Specifies the network address to be joined.	The value is in dotted decimal notation.
network-mask	Specifies the subnet mask of a network address.	The value is in dotted decimal notation.

Default Value

None

View

OSPFv2 route configuration view

Usage Guidelines

One OSPF interface can belong to only one area, but the area can contain multiple interfaces. Before you run this command, if the specified area does not exist, the command automatically creates an area. If the specified interface does not exist, the configuration is still reserved. When the interface appears, an OSPF interface is automatically created.

Example

Configure network segment 2.2.2.0/24 for area 2.

```
switch(config-ospf-1)#network 2.2.2.0 255.255.255.0 area 2
switch(config-ospf-1)#
```

4.4.34 peer priority

Function

The **peer priority** command configures the IPv4 address and priority of an adjacent switch on the NBMA network.
The **no peer** command deletes the IPv4 address of an adjacent switch on the NBMA network.

Format

- **peer** *ipv4-address* **priority** *priority*
- **no peer** *ipv4-address*

Parameters

Parameters	Description	Value
ipv4-address	Specifies the IPv4 address of an adjacent switch.	The value is in dotted decimal notation.
priority	Specifies the priority of a network neighbor.	The value is an integer ranging from 0 to 255.

Default Value

None

View

OSPFv2 route configuration view

Usage Guidelines

If you use this command to set the priority of a peer router, the peer switch must have the same priority as the local switch.

Example

Set the IPv4 address of an adjacent switch on the OSPF network to 10.18.13.1 and priority to 1.

```
switch(config-ospf-1)#peer 10.18.13.1 priority 1
switch(config-ospf-1)#
```

4.4.35 redistribute

Function

The **redistribute** command enables the re-allocation of BGP route, direct route, IS-IS route, and static route.
The **no redistribute** command disables the re-allocation of BGP route, direct route, IS-IS route, and static route.

Format

- **redistribute ospf** *process-id*
- **redistribute** { **static** | **connect** | **rip** | **bgp** | **isis** }
- **redistribute** { **rip** | **isis** | **ospf** } *process-id*
- **no redistribute** { **rip** | **isis** | **ospf** } *process-id*
- **no redistribute** { **static** | **connect** | **rip** | **bgp** | **isis** }
- **no redistribute** { **static** | **connect** | **rip** | **bgp** | **isis** } *dst-address dst-mask*

Parameters

Parameters	Description	Value
static	Re-allocates the static route to the OSPF protocol.	This command is valid only when the static route is introduced if the static route re-allocation is enabled.
ospf	Re-allocates the OSPF routes.	-
connect	Re-allocates the direct route to the OSPF protocol.	This command is valid only when the direct route is introduced.
rip	Re-allocates the RIP route to the OSPF protocol.	This command is valid only when the RIP route is introduced.
bgp	Re-allocates the BGP route to the OSPF protocol	This command is valid only when the BGP route is introduced.
isis	Re-allocates the BGP route to the IS-IS protocol.	This command is valid only when the IS-IS route is introduced.
dst-address	Specifies the destination network address.	The value is in dotted decimal notation.
dst-mask	Specifies the network mask address.	The value is in dotted decimal notation.
process-id	Imports the routes of the specified process.	It is an integer ranging from 1-16

Default Value

None

View

OSPFv2 route configuration view

Usage Guidelines

None.

Example

Configure static route re-allocation.

```
switch(config-ospf-1)#redistribute static
switch(config-ospf-1)#
```

4.4.36 redistribute route-policy

Function

The **redistribute route-policy** command introduces different routing policies.

The **no redistribute route-policy** command clears the introduction to a specified routing policy

Format

- **redistribute** { **static** | **connect** | **rip** | **bgp** | **isis**| **ospf** } **route-policy** *policy-name*
- **no redistribute** { **static** | **connect** | **rip** | **bgp** | **isis** | **ospf** } **route-policy** [*policy-name*]

Parameters

Parameters	Description	Value
static	Configures the policy introducing a static route.	Only routes in compliance with specified routing policy can be introduced. When NAME introduces routes, the routing policy name must be specified. Multiple routing policies can be configured to filter introduced routes of other protocols, in order not to overwrite the pre-configured routing policy. This command is valid only when the static route is introduced if the static route re-allocation is enabled, and the redistribute static command must be configured.
connect	Configures the policy for introducing a direct route.	Only routes in compliance with specified routing policy can be introduced. When NAME introduces routes, the routing policyname must be specified. Multiple routing policies can be configured to filter introduced routes of other protocols, in order not to overwrite the pre-configured routing policy. This command is valid only when the direct route is introduced if the direct route re-allocation is enabled, and the redistribute connect command must be configured.
rip	Configures route measurement for introducing a RIP route.	Only routes in compliance with specified routing policy can be introduced. When NAME introduces routes, the routing policy name must be specified. Multiple routing policies can be configured to filter introduced routes of other protocols, in order not to overwrite the pre-configured routing policy. This command is valid only when the RIP Route is introduced if the RIP route re-allocation is enabled,and the redistribute rip command must be configured.
bgp	Configures the policy for introducing a	Only routes in compliance with specified routing policy can be introduced. When NAME introduces routes, the routing policy name must be specified. Multiple routing policies can be configured to

Parameters	Description	Value
	BGP route.	filter introduced routes of other protocols, in order not to overwrite the pre-configured routing policy. This command is valid only when the BGP route is introduced if the BGP route re-allocation is enabled, and the redistribute bgp command must be configured.
isis	Configures the policy for introducing an IS-IS route.	Only routes in compliance with specified routing policy can be introduced. When NAME introduces routes, the routing policy name must be specified. Multiple routing policies can be configured to filter introduced routes of other protocols,in order not to overwrite the pre-configured routing policy. This command is valid only when the IS-IS route is introduced if the IS-IS route re-allocation is enabled, and the redistribute isis command must be configured
ospf	Configures the routing policy for importing OSPF routes.	Only routes matching specified routing policy can be imported. Name specifies the name of the routing policy for route import. Multiple routing policies can be configured to filter routes imported from other protocols. Later configured routing policies do not override the previously configured ones. Only if the redistribute ospf command is executed to enable the OSPF route re-allocation, can this command take effect when the OSPF routes are imported.
policy-name	Specifies the name of a routing policy.	The value is a string containing no more than 20 bytes.

Default Value

By default, the value is a string of blank characters, indicating that no routing policy is referenced.

View

OSPFv2 route configuration view

Usage Guidelines

None

Example

Configure routing policy 2 for introducing a static route.

```
switch(config-ospf-1)#redistribute static route-policy 2
switch(config-ospf-1)#
```

4.4.37 redistribute metric

Function

The **redistribute metric** command configures OSPF to re-allocate the route and cost learned from the RIP, BGP, Static, and Connect protocols.
The **no redistribute metric** command cancels the re-allocation.

Format

- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** } *dst-network network-mask* **metric** *router-cost* **type** *cost-type*
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** } **metric** *router-cost* **type** *cost-type*
- **no redistribute** { **connect** | **static** | **rip** | **bgp**| **isis** } *dst-network network-mask*

Parameters

Parameters	Description	Value
dst-network	Specifies the destination network address.	The value is in dotted decimal notation.
network-mask	Specifies the network mask address.	The value is in dotted decimal notation.
router-cost	Specifies the route cost.	The value is an integer ranging from 0 to 65535.
cost-type	Specifies the external cost type.	The value is an integer ranging from 0 to 2.

Default Value

By default, OSPF route re-allocation is not configured.

View

OSPFv2 route configuration view

Usage Guidelines

After you use this command, OSPF can advertise routes learned from RIP, BGP, Static, and Connect protocols to the adjacent routers.
By default, all external routes of the same protocol have the same attribute. You can independently specify the cost attribute of a specific route.

Example

Set the route learned from RIP by OSPF through re-allocation to 1.2.3.1, subnet mask to 255.255.255.0, route cost to 10, and cost type to 1.

```
switch(config-ospf-1)#redistribute connect 1.2.3.1 255.255.255.0 metric 10 type 1
switch(config-ospf-1)#
```

4.4.38 redistribute not-advertise|advertise

Function

The **redistribute not-advertise|advertise** command specifies a specific external route to be rejected.

Format

- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** } *dst-network network-mask* { **not-advertise** | **advertise** }

Parameters

Parameters	Description	Value
dst-network	Specifies the destination network address.	The value is in dotted decimal notation.
network-mask	Specifies the network mask address.	The value is in dotted decimal notation.

Default Value

By default, OSPF route re-allocation is not configured.

View

OSPFv2 route configuration view

Usage Guidelines

You can use this command to filter certain external routes.

Example

Set OSPF to reject an external route with protocol isis, address 10.2.3.1, and subnet mask 255.255.255.0.

```
switch(config-ospf-1)#redistribute isis 1 10.2.3.1 255.255.255.0 not-advertise
switch(config-ospf-1)#
```

4.4.39 redistribute range

Function

The **redistribute range** command aggregates re-allocated routes that match the specified network segment.
The **no redistribute range** command deletes the aggregation route entry configured with re-allocation.

Format

- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** } **range** *dst-network network-mask*
- **no redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** } **range** *dst-network network-mask*

Parameters

Parameters	Description	Value

Parameters	Description	Value
static	Configures the policy for introducing a static route.	Only routes in compliance with specified routing policy can be introduced. When NAME introduces routes, the routing policy name must be specified. Multiple routing policies can be configured to filter introduced routes of other protocols, in order not to overwrite the pre-configured routing policy. This command is valid only when the static route is introduced if the static route re-allocation is enabled, and the redistribute static command must be configured.
connect	Configures the policy for introducing a direct route.	Only routes in compliance with specified routing policy can be introduced. When NAME introduces routes, the routing policy name must be specified. Multiple routing policies can be configured to filter introduced routes of other protocols, in order not to overwrite the pre-configured routing policy. This command is valid only when the direct route is introduced if the direct route re-allocation is enabled, and the redistribute connect command must be configured.
rip	Configures route measurement for introducing a RIP route.	Only routes in compliance with specified routing policy can be introduced. When NAME introduces routes, the routing policy name must be specified. Multiple

Parameters	Description	Value
		routing policies can be configured to filter introduced routes of other protocols, in order not to overwrite the pre-configured routing policy. This command is valid only when the RIP route is introduced if the RIP route re-allocation is enabled, and the **redistribute rip** command must be configured.
bgp	Configures the policy for introducing a BGP route.	Only routes in compliance with specified routing policy can be introduced. When NAME introduces routes, the routing policy name must be specified. Multiple routing policies can be configured to filter introduced routes of other protocols, in order not to overwrite the pre-configured routing policy. This command is valid only when the BGP route is introduced if the BGP route re-allocation is enabled, and the **redistribute bgp** command must be configured.
isis	Configures the policy for introducing an IS-IS route.	Only routes in compliance with specified routing policy can be introduced. When NAME introduces routes, the routing policy name must be specified. Multiple routing policies can be configured to filter introduced routes of other protocols, in order not to overwrite the pre-configured routing policy. This command is valid only when the IS-IS

Parameters	Description	Value
		route is introduced if the IS-IS route re-allocation is enabled, and the **redistribute isis** command must be configured.
dst-network	Specifies the destination network address.	The value is in dotted decimal notation.
network-mask	Specifies the network mask address	The value is in dotted decimal notation.

Default Value

By default, the OSPF area does not include any aggregation entry.

View

OSPFv2 route configuration view

Usage Guidelines

None

Example

Configure re-allocated aggregation route entry 10.0.0.0 255.255.0.0.

```
switch(config-ospf-1)#redistribute connect range 10.0.0.0 255.255.0.0
switch(config-ospf-1)#
```

4.4.40 redistribute translate|no-translate

Function

The **redistribute translate|notranslate** command sets the translate bit when NSSA LSA is generated during re-allocation.

Format

- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** } *dst-network network-mask* { **translate** | **no-translate** }
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** } { **translate** | **no-translate** }

Parameters

Parameters	Description	Value
dst-network	Specifies the destination network address.	The value is in dotted decimal notation.
network-mask	Specifies the network mask address.	The value is in dotted decimal notation.

Default Value

By default, OSPF route re-allocation is not configured.

View

OSPFv2 route configuration view

Usage Guidelines

None.

Example

Set the translate bit for OSPF re-allocated isis route with address 10.13.3.1 and mask 255.255.255.0 when NSSA LSA is generated.

```
switch(config-ospf-1)#redistribute isis 10.1.3.1 255.255.255.0 no-translate
switch(config-ospf-1)
```

4.4.41 router-id

Function

The **router-id** command configures the switch ID.

Format

- **router-id** *ip-address*

Parameters

Parameters	Description	Value
ip-address	Specifies the switch ID.	The value is in dotted decimal notation.

Default Value

By default, the switch ID is not configured for the system. During the operation, an IP address of an interface is selected as the switch ID.

View

OSPFv2 route configuration view

Usage Guidelines

The router ID selection rules are as follows:
Minimum static loopback address
Minimum static primary address
Minimum static secondary address
Minimum static link local address
Minimum address allocated by the DHCP

Error return

Example

Set router ID to 1.1.1.1.

```
switch(config-vlanif-3)#ip address 1.1.1.1/24
switch(config-vlanif-3)#quit
switch(config)#router ospf
switch(config-ospf-1)#router-id 1.1.1.1
switch(config-ospf-1)#
```

4.4.42 router ospf

Function

The **router ospf** command enables IPv4 OSPF and enters the OSPF configuration view. The switch supports multi-IPv4 OSPF instances and multi-instance VPN.
The **no router ospf** command disables IPv4 OSPF.

Format

- **router ospf**
- **router ospf** *process-id*
- **no router ospf** [*process-id*]
- **no router ospf**
- **no router ospf all**

Parameters

Parameters	Description	Value
process-id	Specifies IPv4 OSPF process ID.	The value is an integer ranging from 1 to 16. If the instance ID is not entered, the instance ID is 1 by default.

Default Value

By default, the system disables IPv4 OSPF.

View

Global configuration view

Usage Guidelines

Before running this command, you must run the ip address command to configure the IP address of the VLAN interface.

Example

Enable OSPF on the switch.

```
switch(config-vlanif-3)#ip address 1.1.1.1/24
switch(config-vlanif-3)#quit
switch(config)#router ospf
switch(config-ospf-1)#
```

4.4.43 reset ospf

Function

The **reset ospf** command restarts the OSPF process.

Format

- **reset ospf**
- **reset ospf** *process-id*

Parameters

Parameters	Description	Value
process-id	Specifies the OSPF process ID.	The value is an integer ranging from 1 to 16.

Default Value

None

View

Global configuration view, OSPFv2 route configuration view

Usage Guidelines

None

Example

Restart OSPF process 1.

```
switch(config-ospf-1)#reset ospf 1
switch(config-ospf-1)
```

4.4.44 reset ospf counters

Function

The **reset ospf counters** command zeros the OSPF counter.

Format

- **reset ospf counters**
- **reset ospf** *process-id* **counters**

Parameters

Parameters	Description	Value
process-id	Specifies the OSPF process ID.	The value is an integer ranging from 1 to 16.

Default Value

None.

View

Global configuration view, OSPFv2 route configuration view

Usage Guidelines

None

Example

Zero the OSPF counter.

```
switch(config-ospf-1)#reset ospf counters
switch(config-ospf-1)#
```

4.4.45 spf-running-interval

Function

The **spf-running-interval** command configures the interval for route calculation.

Format

- **spf-running-interval** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	Specifies the interval for route calculation.	The value is an integer ranging from 1 to 60, in ms.
default	Specifies the default interval for route calculation.	2

Default Value

2

View

OSPFv2 configuration view

Usage Guidelines

The OSPF database synchronization and route calculation do not have a direct cause-effect relation. The device cannot learn whether the database synchronization is complete. It checks the synchronization based on the specified calculation interval. If it determines route calculation is required, it starts to calculate the route. A complete calculation process is time-consuming. If the network keeps updating the database the route calculation persists. Therefore, you can set the interval for route calculation to a larger value to reduce the device burden,
The OSPF route does not need to be re-calculated at the end of each interval. It is calculated only when change occurs. Therefore, when the network is stable, the interval for route calculation does not affect OSPF performance.

Example

Set the interval for route calculation to 30 ms.

```
switch(config-ospf-1)#spf-running-interval 30
switch(config-ospf-1)#
```

4.4.46 show ip ospf area

Function

The **show ip ospf area** command shows all areas directly connected with the switch.

Format

- **show ip ospf area** [*area-id*]
- **show ip ospf area process** *process-id*

Parameters

Parameters	Description	Value
[area-id]	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
process-id	Specifies the process ID.	The value is an integer ranging from 1 to 16.

Default Value

None

View

Common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, and Loopback interface configuration view

Usage Guidelines

You can use this command to learn whether the OSPF area is correctly set and perform OSPF fault locating.

Example

Display all areas directly connected with the switch.

```
switch#show ip ospf area
AreaId          Flag(Hex) RouteUpdates      ABR    ASBR   LSA Count
1               8         1                 0      0      0
```

4.4.47 show ip ospf bfd session

Function

The **show ip ospf bfd session** command shows BFD neighbor information.

Format

- **show ip ospf bfd session**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, and Loopback interface configuration view

Usage Guidelines

None

Example

Display BFD neighbor information.

```
switch#show ip ospf bfd session
OSPF Process 1
Neighbor : 1.1.1.2        NeighborId : 1.1.1.2
  Interface : ge1/0/1             BFDState : up
Min TX : 200      Min RX : 200
Multiplier : 3       BFD Local Dis : 1
LocalIpAdd : 1.1.1.1 RemoteIpAdd : 1.1.1.2
  Diagnostic Info : noDiagnostic
switch#
```

4.4.48 show ip ospf brief

Function

The **show ip ospf brief** command shows OSPF global Parameters information.

Format

- **show ip ospf brief**
- **show ip ospf brief process** *process-id*

Parameters

Parameters	Description	Value
process-id	Specifies the process ID.	The value is an integer ranging from 1 to 16.

Default Value

None

View

Common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, and Loopback interface configuration view

Usage Guidelines

You can use this command to learn whether the OSPF area is correctly set and perform OSPF fault locating.

Example

Display all areas directly connected with the switch.

```
switch(config-ospf-1)#show ip ospf brief
OSPF Instance 1

OSPF General Parameters
Admin Status     :enable
Vpn Name :N/A
Valid Ttl     0
Router ID   :10.18.13.200
Version      2
Area Border Router     :false
AS Border Router       :false
External LSA Count     0
External LSA Checksum Sum        0
TOS Support      :false
New LSA Received      0
```

```
External LSDB Limit     :-1 No Limited
Exit Overflow Interval  0
Opaque enable   :no
Redistribute local enable     :no
Redistribute bgp enable       :no
Redistribute isis enable      :no
switch(config-ospf-1)#
```

4.4.49 show ip ospf config

Function

show ip ospf config command is used to display information of OSPF protocol operation.

Format

- **show ip ospf config**

Parameters

None

Default Value

None

View

Privilege User View, Global Configuration View, Common User View, OSPFv2 Route Configuration View, VLANIF Configuration View, LoopbckInterface Configuration View

Usage Guidelines

The input of the command is able to check whether the OSPF protocol is correctly configured so that to process OSPF failure check.

Example

Display overall OSPF running information.

```
switch(config)#show ip ospf config
!!Ospf Configuration
 router ospf 1
 router-id 10.18.13.200
switch(config)#
```

4.4.50 show ip ospf database

Function

The **show ip ospf database** command shows OSPF database information.

Format

- **show ip ospf database**
- **show ip ospf database area** *area-id*
- **show ip ospf database area** *area-id* **process** *process-id*
- **show ip ospf database** { **as-external-lsa** | **type9** | **type11** } *Ls-id adverrouter-id*
- **show ip ospf database** { **as-external-lsa** | **type9** | **type11** } *Ls-id adverrouter-id process-id*
- **show ip ospf database** { **router** | **network** | **summary-network** | **summary-asbr** | **as-external-lsa** | **nssa-lsa** | **type9** | **type10** | **type11** }
- **show ip ospf database** { **router** | **network** | **summary-network** | **summary-asbr** | **as-external-lsa** | **nssa-lsa** | **type9** | **type10** | **type11** } **process** *process-id*
- **show ip ospf database** { **router** | **network** | **summary-network** | **summary-asbr** | **nssa-lsa** | **type10** } *LS-id adverrouter-id area-id*
- **show ip ospf database** { **router** | **network** | **summary-network** | **summary-asbr** | **nssa-lsa** | **type10** } *LS-id adverrouter-id area-id process-id*
- **show ip ospf database age** *min-age max-age*
- **show ip ospf database age** *min-age max-age* **count**
- **show ip ospf database count**
- **show ip ospf database count process** *process-id*
- **show ip ospf database expire**
- **show ip ospf database expire count**
- **show ip ospf database expire process** *process-id*
- **show ip ospf database process** *process-id*
- **show ip ospf database total count**

Parameters

Parameters	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IP address. The value ranges from 0 to 4294967295.
LS-id	Specifies an LS ID.	The value is in dotted decimal notation.
adverrouter-id	Specifies the advertising route ID.	The value is in dotted decimal notation.
router | network | summary-network | summary-asbr | as-external-lsa | nssa-lsa | type9 | type10 | type11	Specifies the LSA type.	-

Parameters	Description	Value
process-id	Specifies the process ID.	The value is an integer ranging from 1 to 16.
min-age	Specifies the minimum database aging time.	The value is an integer ranging from 0 to 3600.
max-age	Specifies themaximum database aging time.	The value is an integer ranging from 0 to 3600.
string	Specifies a character string used for filtering the configuration information to be displayed.	The value is a character string.

Default Value

None

View

Common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, and Loopback interface configuration view

Usage Guidelines

You can use this command to view information about the OSPF link state database, helping you implement fault diagnosis.

Example

Display the OSPF database information.

```
switch#sho ip ospf database network
        Database of OSPF Instance 1


                        Network LSA (area 0)
        LinkId          ADV Router      Age     Seq#       CheckSum  Len
        3.2.1.2         172.17.1.250    1399    0x80000005 0x2638    32
switch#
```

4.4.51 show ip ospf graceful-restart

Function

The **show ip ospf graceful-restart** command shows information about OSPF graceful restart of the switch.

Format

- **show ip ospf graceful-restart**

Parameters

None

Default Value

None

View

Privilege User View, Global Configuration View, Common User View, OSPFv2 Route Configuration View, VLANIF Configuration View, LoopbckInterface Configuration View

Usage Guidelines

None

Example

#Display information about OSPF graceful restart of the switch.

```
switch(config-vlanif-3)#show ip ospf graceful-restart
OSPF Instance 1
Restart Capability            : Not Support
Restart Helper Capability     : Not Support
Restart State                 : Not in Restarting
Restart Period                : 120 second
Restart Exit Reason           : none
Restart Age                   : 50
switch(config-vlanif-3)#
```

4.4.52 show ip ospf interface

Function

The **show ip ospf interface** command shows information about OSPF interface table of the switch.

Format

- **show ip ospf interface** [*ip-address*]
- **show ip ospf interface count**

Parameters

Parameters	Description	Value
[ip-address]	Specifies the IP address of an interface. It is optional.	The value is in dotted decimal notation.

Default Value

None

View

Common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, and Loopback interface configuration view

Usage Guidelines

You can use this command to learn OSPF running situations of the interface, check whether configuration is correct, and determine whether OSPF fault identification is performed.

Example

Display information about OSPF interface table of the switch.

```
switch#show ip ospf interface
OSPF Process 1
 Interface        IpAddr          AreaId          State           Cost
 vlan 14          10.0.14.1       0               down            1
 OSPF Process 2
 Interface        IpAddr          AreaId          State           Cost
 vlan 10          10.0.10.1       0               designatedRouter 1
switch#
```

4.4.53 show ip ospf neighbor

Function

The **show ip ospf neighbor** command shows information about the adjacent station table of the switch.

Format

- **show ip ospf neighbor** [*ip-address*]
- **show ip ospf neighbor process** *process-id*
- **show ip ospf neighbor state count**
- **show ip ospf neighbor state statistic**
- **show ip ospf neighbor state statistic process** *process-id*

Parameters

Parameters	Description	Value
[ip-address]	Specifies the IP address of a neighbor. It is optional.	The value is in dotted decimal notation.
process-id	Specifies the process ID.	The value is an integer ranging from 1 to 16.

Default Value

None

View

Common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, and Loopback interface configuration view

Usage Guidelines

You can use this command to learn OSPF running situations of the interface, check whether configuration is correct, and determine whether OSPF fault identification is performed.

Example

Display information about the adjacent station table of the switch.

```
switch#show ip ospf neighbor
                                OSPF Instance 1
 IpAddress          NeighborID          Option    Priority  State          Event    Aging
  201.1.1.2          192.0.2.1            2          0        full           6        37
  202.1.1.2         192.0.1.1            2          0        full           6        30
switch#
```

4.4.54 show ip ospf route

Function

The **show ip ospf route** command shows the OSPF routing information.

Format

- **show ip ospf route**
- **show ip ospf route process** *process-id*

Parameters

Parameters	Description	Value
process-id	Specifies the process ID.	The value is an integer ranging from 1 to 16.
string	Specifies a character string used for filtering the configuration information to be displayed.	The value is a character string.

Default Value

None

View

Common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, and Loopback interface configuration view

Usage Guidelines

None

Example

Display OSPF routing information.

```
switch#show ip ospf route
OSPF Process 1
 RoutType   Prefix        hType      Cost      Cost2      NextHop        ackupNextHop       AreaId
 ASBR       1.1.1.1/32    INTRA        1          0          1.1.1.1          0.0.0.0            1
 Network 1.1.1.0/24    INTRA        1        0              1.1.1.2          0.0.0.0            N/A
 Network    10.1.1.0/24        ASE2          1          1      1.1.1.1          0.0.0.0            N/A
 Network 100.1.1.0/24       ASE2          1          1      1.1.1.1          0.0.0.0            N/A
switch#
```

4.4.55 show ip ospf route count

Function

The **show ip ospf route count** command shows the OSPF route quantity.

Format

- **show ip ospf route count**
- **show ip ospf route count process** *process-id*
- **show ip ospf route total count**

Parameters

Parameters	Description	Value
process-id	Specifies the process ID.	The value is an integer ranging from 1 to 16.
string	Specifies a character string used for filtering the configuration information to be displayed.	The value is a character string.

Default Value

None

View

Common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, and Loopback interface configuration view

Usage Guidelines

None

Example

Display OSPF routing information.

```
switch#show ip ospf route count
ABR   ASBR   Network   Intra   Inter   External
4     5      3         0       0       0

switch#
```

4.4.56 show ip ospf statistic bfd

Function

The **show ip ospf statistic bfd** command shows statistics, including the BFD, global, interface, ISA, neighbor, and SPF information.

Format

- **show ip ospf statistic bfd**
- **show ip ospf statistic bfd** *start-item*

Parameters

Parameters	Description	Value
start-item	Specifies the BFD statistics corresponding to the SN.	The value is an integer ranging from 1 to 3000.

Default Value

None

View

Common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, and Loopback interface configuration view

Usage Guidelines

None

Example

View the statistics of BFD status change.

```
switch#show ip ospf statistic bfd
process time                    nbr addr        state       diag
 1       2019/11/19 06:09:31 20.1.1.2        Down          neighbor signaled session down

 1       2019/11/19 06:09:56 20.1.1.2        Down          neighbor signaled session down
```

```
switch#
```

4.4.57 show ip ospf statistic global

Function

The **show ip ospf statistic global** command displays the global statistics of the OSPF protocol.

Format

- **show ip ospf statistic global**

Parameters

None

Default Value

None

View

Common user view, priviledge user view, global configuration view, OSPFv2 routing configuration view, VLANIF configuration view and Loopback interface configuration view

Usage Guidelines

None

Example

View the global statistics of the OSPF protocol.

```
switch#show ip ospf statistic global
 OSPF Global Statistic

 Working Mode:NOMAL
 RawSocket     :160    RouteSocket :161

 Memory Statistics
 Configuration Params
 Process    : 16
 Interface: 32
 Neighbor : 64
 Area        : 32
 LSA         : 5000
 Route       : 4000

 OSPF System Statistics
 kernel Route Table Statistic
```

```
System Route Add: Success: 0                Failed: 0
System Route Del: Success: 0                Failed: 0
Backup Route Add: Success: 0                Failed: 0
Backup Route Del: Success: 0                Failed: 0               Not Need Del: 0
System Error
Current Errno: 0 Normal Errno: 0 Normal Error Count: 0
Last Error Route
Rtsock: 0 Vrid: 0 Rt Add: 0 Dest: 0/0 Fwd: 0 Metric: 0

Hardware Route Table Statistic
Route Msg                       : Success       : 2             Failed: 0
Route Msg route add cnt: Total Add    : 3               Add Failed: 0
Route Msg route del cnt: Total Del    : 3               Del Failed: 0
Route Msg route cnt      : Total Sucess: 6
Route Msg Errorno        : Errorno       : 0

RTM Msg RX Statistic
RTM IfAddr Add: 4               RTM IfAddr Del: 0               RTM IfInfo : 0
RTM New Msg    : 0              New Msg Add    : 0              New Msg Del: 0
RTM Add          : 5            RTM Del          : 3

Pkt To Cpu Errcnt: 0
Mutigroup Errcnt : 0 Errno: 0

OSPF Sync Statistics
TxPktcnt: 0             RcvPktcnt: 0
TxLsa    : 0            TxOldLsa : 0
RxLsa    : 0            RxOldLsa : 0            RxError: 0
Sync Message Statistics
syn type        send            rcv
process         0               0
area            0               0
if              0               0
nbr             0               0
lsa             0               0
lsaFragement    0               0
lsa rsmt        0               0
seq mismatch packet:0, time:

Avl Api Usage Statistic
GetFirst Count: 21583       Lookup Count: 15303       Add Count: 502       Delete Count: 168
```

```
Total Packet Statistics
              Rcv pkt    Send pkt   Rcv bytes    Send bytes   Rcv Lsa    Send Lsa
 HELLO        12731      16963      865700       797324       0          0
 DD           5          7          340          384          4          8
 REQUEST      2          2          184          96           8          4
 UPDATE       287        330        24264        22236        291        336
 ACK          265        213        18320        10872        333        288

Total Discard       : 0             Total Rxd       : 13290       Total Txd            : 17515
Init DD Retransmit: 1               DD Retransmit : 0             Request Retransmit: 0
Nbr Rxmt Count      : 0             BFD Admin Down: 0             BFD Nbr Down         : 0
Rxd Unicast         : 17            Rxd Multicast : 13273
Txd Unicast         : 14            Txd Multicast : 17501
Mcast Update        : 325           Ucast Update  : 5

LSA Check Statistics
Originate Router Isa Count: 0 Originate Network Lsa Count: 0

Count of Local Lsa Originate
 Type        Build       Changed
 1           17          6
 2           4           0
 4           1           0
Count of Received Lsa
 Type   Rxd       MoreRecent   LessRecent   SameRecent   BodyChanged
 1      113       111          0            2            8
 2      108       105          0            3            5
 5      70        67           0            3            4

switch#
```

4.4.58 show ip ospf statistic interface

Function

The **show ip ospf statistic interface** command displays the statistics of an OSPF interface.

Format

- **show ip ospf statistic interface** *ip-address*

Parameters

Parameters	Description	Value
ip-address	Specifies the IP address of an interface.	The value is in dotted decimal notation.

Default Value

None

View

Common user view, priviledge user view, global configuration view, OSPFv2 routing configuration view, VLANIF configuration view and Loopback interface configuration view

Usage Guidelines

None

Example

View the statistics of an OSPF interface.

```
switch#show ip ospf statistic interface 1.1.1. 2
OSPF Process 1
 Interface 100ge1/0/1 Statistics information:
 ------------------------------------------------
 IP address                    :1.1.1.2
 Area ID                       :1
 Ifnet Unit                    :2
 Vrid                          :0
              Rcv pkt    Send pkt   Rcv bytes    Send bytes   Rcv Lsa    Send Lsa
 HELLO        0          0          0            0            0          0
 DD           0          0          0            0            0          0
 REQUEST      0          0          0            0            0          0
 UPDATE       0          0          0            0            0          0
 ACK          0          0          0            0            0          0
 rcv packet total count        :0
 send packet total count       :0
 Rxd Unicast                   :0
 Rxd Multicast                 :0
 Txd Unicast                   :0
 Txd Multicast                 :0
 Init DD Retransmit            :0
 DD Retransmit                 :0
```

```
Mcast Update                    :0
Ucast Update                    :0
- Request Retransmit            :0
Packet from invalid source   :0
Packet from unkown neighbor :0
Packet with error auth type :0(last 0)
Packet with error auth info :0
Bad network mask in Hello    :0(last 0)
Bad hello interval in hello :0(last 0)
Bad dead interval in hello   :0(last 0)
Bad External bit in hello    :0
Bad NSSA bit in hello        :0
Neighbor negodone            :0
Neighbor exchange done       :0
Neighbor bad lsa request     :0
Neighbor loading done        :0
Neighbor sequence mismatch   :0
Neighbor shutdown or timeout:0
Interface up times           :0
Interface down times         :0
Interface neighbor changed   :0
Mismatch MTU in DD packet    :0(last 0)
switch#
```

4.4.59 show ip ospf statistic lsa

Function

The **show ip ospf statistic lsa** command displays the LSA generation statistics of OSPF.

Format

- **show ip ospf statistic lsa**
- **show ip ospf statistic lsa** *start-item*

Parameters

Parameters	Description	Value
start-item	Displays the starting index of the statistics.	It is an integer ranging from 1 to 3000.

Default Value

None

View

Common user view, priviledge user view, global configuration view, OSPFv2 routing configuration view, VLANIF configuration view and Loopback interface configuration view

Usage Guidelines

None

Example

View the LSA generation statistics of OSPF.

```
switch#show ip ospf statistic lsa
 process time                  t id          adv           seqnum     age   len   action
 1       2019/02/22 13:11:32 1 1.1.1.2       1.1.1.2       80000001   0     36    add
 1       2019/02/22 13:12:19 1 1.1.1.1       1.1.1.1       80000002   5     36    add
 1       2019/02/22 13:12:52 1 1.1.1.2       1.1.1.2       80000002   0     36    mod
 1       2019/02/22 13:12:52 2 1.1.1.2       1.1.1.2       80000001   0     32    add
 1       2019/02/22 13:12:52 1 1.1.1.1       1.1.1.1       80000003   1     36    mod
 1       2019/02/22 13:16:45 1 1.1.1.2       1.1.1.2       80000003   0     36    mod
 1       2019/02/22 13:16:47 1 1.1.1.1       1.1.1.1       80000003   3600  36    del
 1       2019/02/22 13:16:47 2 1.1.1.2       1.1.1.2       80000001   3600  32    del
 1       2019/02/22 13:16:59 1 1.1.1.1       1.1.1.1       80000004   15    36    add
 1       2019/02/22 13:17:07 1 1.1.1.2       1.1.1.2       80000004   0     36    mod
switch#
```

4.4.60 show ip ospf statistic memory

Function

The **show ip ospf statistic memory** command displays the OSPF memory statistics.

Format

- **show ip ospf statistic memory**

Parameters

None

Default Value

None

View

Common user view, priviledge user view, global configuration view, OSPFv2 routing configuration view, VLANIF configuration view and Loopback interface configuration view

Usage Guidelines

None

Example

View the OSPF memory statistics.

```
switch#show ip ospf statistic memory

Detailed Memory Operation:
Index    Add      Fail     Free     Current  Size     Description
0        0        0        0        0        0
1        0        0        0        0        0
2        0        0        0        0        0
3        0        0        0        0        0
4        0        0        0        0        0
5        0        0        0        0        0
6        0        0        0        0        0
7        0        0        0        0        0
8        0        0        0        0        0
9        0        0        0        0        0
10       0        0        0        0        0
11       0        0        0        0        0
12       0        0        0        0        0
13       0        0        0        0        0
14       0        0        0        0        0
15       0        0        0        0        0
16       0        0        0        0        0
17       0        0        0        0        0
18       0        0        0        0        0
19       0        0        0        0        0
20       0        0        0        0        0
21       0        0        0        0        0
22       0        0        0        0        0
23       0        0        0        0        0
24       0        0        0        0        0
25       0        0        0        0        0
26       0        0        0        0        0


Detailed Total Memory Operation:
Index    Add      Fail     Free     Current  Size     Description
```

0	0	0	0	0	0
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	0	0
7	0	0	0	0	0
8	0	0	0	0	0
9	0	0	0	0	0
10	0	0	0	0	0
11	0	0	0	0	0
12	0	0	0	0	0
13	0	0	0	0	0
14	0	0	0	0	0
15	0	0	0	0	0
16	0	0	0	0	0
17	0	0	0	0	0
18	0	0	0	0	0
19	0	0	0	0	0
20	0	0	0	0	0
21	0	0	0	0	0
22	0	0	0	0	0
23	0	0	0	0	0
24	0	0	0	0	0
25	0	0	0	0	0
26	0	0	0	0	0

switch#

4.4.61 show ip ospf statistic neighbor

Function

The **show ip ospf statistic neighbor** command displays the OSPF neighbor status statistics.

Format

- **show ip ospf statistic neighbor**
- **show ip ospf statistic neighbor** *start-item*

Parameters

Parameters	Description	Value
start-item	Displays the starting index of	It is an integer ranging from 1 to 3000.

Parameters	Description	Value
	the statistics.	

Default Value

None

View

Common user view, priviledge user view, global configuration view, OSPFv2 routing configuration view, VLANIF configuration view and Loopback interface configuration view

Usage Guidelines

None

Example

View the OSPF neighbor status statistics.

```
switch#show ip ospf statistic neighbor
 process time                    nbr_addr          last_state   state      event
 1       2019/02/22 13:11:42 1.1.1.1           Down          Init       hello-rcvd
 1       2019/02/22 13:11:44 1.1.1.1           Init          2-way      2-way
 1       2019/02/22 13:12:15 1.1.1.1           2-way         ExStart    Adj-OK
 1       2019/02/22 13:12:15 1.1.1.1           ExStart       Exchange   neg-done
 1       2019/02/22 13:12:15 1.1.1.1           Exchange      Loading    exchange-done
 1       2019/02/22 13:12:52 1.1.1.1           Loading       Full       loading-done
 1       2019/02/22 13:16:45 1.1.1.1           Full          Down       Expired
switch#
```

4.4.62 show ip ospf statistic route

Function

The **show ip ospf statistic route** command displays the OSPF routing statistics.

Format

- **show ip ospf statistic route**

Parameters

None

Default Value

None

View

Common user view, priviledge user view, global configuration view, OSPFv2 routing configuration view, VLANIF configuration view and Loopback interface configuration view

Usage Guidelines

None

Example

View the OSPF routing statistics.

```
switch#show ip ospf statistic route

 OSPF Process 1

                              SPF Table (area 1)
 type       id               nexthop          cost     ifunit     parent                role
 router     1.1.1.2          N/A              0        0          N/A                   main

                            Network Route Table
 type       dest             nexthop          cost     ifunit     role
 INTRA      1.1.1.0/24       1.1.1.2          1        2          main
switch#
```

4.4.63 show ip ospf statistic route process

Function

The **show ip ospf statistic route process** command displays the OSPF routing statistics of a specified instance.

Format

- **show ip ospf statistic route process** *process-id*

Parameters

Parameters	Description	Value
process-id	Specifies the OSFP instance number.	It is an integer ranging from 1 to 16.

Default Value

None

View

Common user view, priviledge user view, global configuration view, OSPFv2 routing configuration view, VLANIF configuration view and Loopback interface configuration view

Usage Guidelines

None

Example

View the OSPF routing statistics of a specified instance.

```
switch#show ip ospf statistic route process 1

 OSPF Process 1

                          SPF Table (area 1)
 type       id            nexthop          cost    ifunit    parent          role
 router     1.1.1.2       N/A              0       0         N/A             main

                          Network Route Table
 type       dest          nexthop          cost    ifunit    role
 INTRA      1.1.1.0/24    1.1.1.2          1       2         main
switch#
```

4.4.64 show ip ospf statistic spf

Function

The **show ip ospf statistic spf** command displays the starting index of the SPF statistics of OSPF.

Format

- **show ip ospf statistic spf**
- **show ip ospf statistic spf** *start-item*

Parameters

Parameters	Description	Value
start-item	Displays the starting index of the SPF statistics.	It is an integer ranging from 1 to 3000.

Default Value

None

View

Common user view, priviledge user view, global configuration view, OSPFv2 routing configuration view, VLANIF configuration view and Loopback interface configuration view

Usage Guidelines

None

Example

Display the starting index of the SPF statistics of OSPF.

```
switch#show ip ospf statistic spf
 process spf_start_time          calc(spf/ia/ase)   route/abr/asbr callspf
 1       2019/02/22 13:11:32 0(0/0/0)               1/0/0          0
 1       2019/02/22 13:12:19 0(0/0/0)               1/0/0          0
 1       2019/02/22 13:12:52 0(0/0/0)               0/0/0          0
 1       2019/02/22 13:12:52 0(0/0/0)               1/0/0          0
 1       2019/02/22 13:12:52 0(0/0/0)               3/0/1          3
 1       2019/02/22 13:16:45 0(0/0/0)               1/0/0          0
 1       2019/02/22 13:16:47 0(0/0/0)               1/0/0          0
 1       2019/02/22 13:16:47 0(0/0/0)               1/0/0          0
 1       2019/02/22 13:16:56 0(0/0/0)               1/0/0          3
 1       2019/02/22 13:16:59 0(0/0/0)               1/0/0          3
switch#
```

4.4.65 show ip ospf trap

Function

The **show ip ospf trap** command shows information about the configured Trap.

Format

- **show ip ospf trap**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, and Loopback interface configuration view

Usage Guidelines

None

Example

Display information about the configured Trap.

```
switch#show ip ospf trap
 ------------------------------------------------------------
```

```
OSPF Process 1
Trap number : 20
------------------------------------------------------------
Trap name                                Status        Excessive Flag
ospfvirtifstatechange                    off           N
ospfnbrstatechange                       off           N
ospfvirtnbrstatechange                   off           N
ospfifconfigerror                        off           Y
ospfvirtifconfigerror                    off           Y
ospfifauthfailure                        off           N
ospfvirtifauthfailure                    off           N
ospfifrxbadpacket                        off           N
ospfvirtifrxbadpacket                    off           N
ospftxretransmit                         off           Y
ospfvirtiftxretransmit                   off           Y
ospforiginatelsa                         off           Y
ospfmaxagelsa                            off           Y
ospflsdboverflow                         off           N
ospflsdbapproachingoverflow              off           N
ospfifstatechange                        off           N
ospfnssatranslatorstatuschange           off           N
ospfrestartstatuschange                  off           N
ospfnbrrestarthelperstatuschange         off           N
ospfvirtnbrrestarthelperstatuschange     off           N
switch#
```

4.4.66 show ip ospf vitual interface

Function

The **show ip ospf vitual interface** command shows the interface of a configured virtual link.

Format

- **show ip ospf vitual interface**
- **show ip ospf vitual interface process** *process*-id
- **show ip ospf virtual interface** *(A.B.C.D) (A.B.C.D)*
- **show ip ospf virtual interface** *virtual-interface-area-id1 virtual-interface-area-id2*

Parameters

Parameters	Description	Value
virtual-interface-area-id1	Specifies a transit area ID.	The value is a decimal number ranging from 0 to 4294967295.

Parameters	Description	Value
virtual-interface-area-id2	Virtual link neighbor route-id.	The value is in dotted decimal notation.
(A.B.C.D) (A.B.C.D)	Specifies the ip address.	The value is in dotted decimal notation.
process-id	Specifies the process ID.	The value is an integer ranging from 1 to 16.

Default Value

None

View

Common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view

Usage Guidelines

None

Example

Display the virtual link interface.

```
switch#show ip ospf virtual interface
OSPF Process 1
Area NeighborId     State
1    2.1.1.2        pointToPoint
switch#
```

4.4.67 show ip ospf virtual neighbor

Function

show ip ospf vitual neighbor command is used to display virtual neighbor information in virtual-link configured by the user.

Format

- **show ip ospf vitual neighbor**
- **show ip ospf vitual neighbor process** *process-id*

Parameters

Parameters	Description	Value
process-id	Process ID	integer, 1-16

Default Value

None

View

Common User View, Privilege User View, Global Configuration View, OSPFv2 Route Configuration View, VLANIF Configuration View

Usage Guidelines

None

Example

Display the OSPF virtual neighbor.

```
switch#show ip ospf virtual neighbor
OSPF Process 1
 ------------------------------------------------
 Neighbor Address                 :0.0.0.0
 Neighbor Id                      :2.1.1.2
 Neighbor State                   :Full
 Neighbor Event Count             :8
 Neighbor Retransmit Queue Length :0
 Neighbor Options                 :0
switch#
```

4.4.68 snmp-trap

Function

The **snmp-trap** command enables or disables the OSPF Trap alarm.

Format

- **snmp-trap** { **enable** / **disable** }
- **snmp-trap** { **enable** | **disable** } **trap-name** { **ospfifauthfailure** | **ospfifconfigerror** | **ospfifrxbadpacket** | **ospfifstatechange** | **ospflsdbapproachingoverflow** | **ospflsdboverflow** | **ospfmaxagelsa** | **ospfnbrrestarthelperstatuschange** | **ospfnbrstatechange** | **ospfnssatranslatorstatuschange** | **ospforiginatelsa** | **ospfrestartstatuschange** | **ospftxretransmit** | **ospfvirtifauthfailure** | **ospfvirtifconfigerror** | **ospfvirtifrxbadpacket** | **ospfvirtifstatechange** | **ospfvirtiftxretransmit** | **ospfvirtnbrrestarthelperstatuschange** | **ospfvirtnbrstatechange** }

Parameters

Parameters	Description	Value
enable	Enables the OSPF Trap alarm.	-
disable	Disables the OSPF Trap alarm.	-

Default Value

Disable

View

OSPFv2 configuration view

Usage Guidelines

None

Example

Enable SNMP Trap

```
switch(config-ospf-1)#snmp-trap enable
switch(config-ospf-1)#
```

4.4.69 opaque

Function

The **opaque** command enables or disables the opaque function.

Format

- **opaque** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the opaque function.	-
disable	Disables the opaque function.	-

Default Value

By default, the opaque function is disabled

View

OSPFv2 route configuration view

Usage Guidelines

You can use this command to enable or disable the opaque function. If the opaque function is enabled, the protocol module can process link state notifications of types 9, 10, and 11. If the opaque function is disabled, the protocol module does not process link state notifications of these types.

Example

Enable the opaque function.

```
switch(config-ospf-1)#opaque enable
switch(config-ospf-1)#
```

4.4.70 bandwidth-reference

Function

The **bandwidth-reference** command configures the reference bandwidth of an interface, used to dynamically calculate the interface cost.

Format

- **bandwidth-reference** { *bandwidth* | **default** }

Parameters

Parameters	Description	Value
bandwidth	Specifies the range of reference rate.	The value is an integer ranging from 1 to 100000.
default	default	By default, the reference link cost is 100M.

Default Value

By default, the reference link cost is 100M.

View

OSPFv2 route configuration view

Usage Guidelines

None

Example

Set the reference bandwidth of an interface to 1000.

```
switch(config-ospf-1)#bandwidth-reference 1000
switch(config-ospf-1)#
```

4.4.71 default-route-advertise always

Function

The **default-route-advertise always** command notifies the common OSPF route area of the default route, that is, forcibly advertising the default route to the OSPF route area. The switch generates and publishes a Category-5 LSA describing the default route. In addition, the switch does not calculate default routes of other devices.
The **no default-route-advertise** command cancels the notification to the common OSPF route area of the default route.

Format

- **default-route-advertise always**
- **default-route-advertise always cost** *cost-value*
- **default-route-advertise always cost** *cost-value* **type** *type-value*
- **default-route-advertise always type** *type-value*
- **no default-route-advertise**

Parameters

Parameters	Description	Value
cost-value	Specifies the overhead of the imported default routes.	It is an integer ranging from 1 to 65535.
typp-value	Specifies the type of the imported default routes.	It is an integer ranging from 1 to 2.

Default Value

By default, default-route-advertise always is disabled.

View

OSPFv2 route configuration view

Usage Guidelines

None

Example

Configure the switch to advertise the default route to the common OSPF route area.

```
switch(config-ospf-1)#default-route-advertise always
switch(config-ospf-1)#
```

4.4.72 loop-prevent

Function

The **loop-prevent** command enables or disables the DN bit check to avoid route loop.

Format

- **loop-prevent** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables DN bit check.	-
disable	Disables DN bit check.	-

Default Value

By default, loop-prevent is disabled.

View

OSPFv2 configuration view

Usage Guidelines

In OSPF multi-VPN instance, if the DN bit is set in Type3, Type5, or Type7 LSA and the loop-prevent is enabled, the OSPF route is not calculated.

Example

Enable loop-prevent.

```
switch(config-ospf-1)#loop-prevent enable
switch(config-ospf-1)#
```

4.4.73 frr {enable|disable}

Function

The **frr {enable|disable}** command enables or disables the fast re-route function.

Format

- **frr** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	enable the fast re-route function	-
disable	disable the fast re-route function	-

Default Value

disable

View

OSPFv2 route configuration view

Usage Guidelines

In OSPF multi-VPN instance, if the DN bit is set in Type3, Type5, or Type7 LSA and the loop-prevent is enabled, the OSPF route is not calculated..

Example

Enable the fast re-route function.

```
switch(config-ospf-1)#frr enable
switch(config-ospf-1)#
```

4.4.74 rfc1583 compatible

Function

The **rfc1583 compatible** command enables or disables preferential route selection rules compatible with RFC1583.

Format

- **rfc1583 compatible** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enable the RFC1583 compatible function.	-
disable	Disable the RFC1583 compatible function.	-

Default Value

By default, the preferential route selection rules compatible with RFC1583 are disabled.

View

OSPFv2 configuration view

Usage Guidelines

None

Example

Enable preferential route selection rules compatible with RFC1583.

```
switch(config-ospf-1)#rfc1583 compatible enable
switch(config-ospf-1)#
```

4.4.75 route-tag

Function

The **route-tag** command configures the tag for a route introduced by the VPN

Format

- **route-tag** { *tag* | **default** }

Parameters

Parameters	Description	Value

Parameters	Description	Value
tag	Specifies the tag for a route introduced by the VPN.	The value is an integer ranging from 1 to 65535.
default	Disables loop detection using a tag.	-

Default Value

None

View

OSPFv2 configuration view

Usage Guidelines

None

Example

Set route-tag of OSPF process 1001 to 1000.

```
switch(config-ospf-1)#route-tag 1000
switch(config-ospf-1)#
```

4.4.76 preference

Function

The **preference** command configures the priority of OSPF routes.
The **no preference** command deletes the priority configuration of OSPF routes.

Format

- **preference** *priority*
- **preference** *priority* **route-policy** *route-policy-name*
- **no preference**

Parameters

Parameters	Description	Value
priority	Specifies the priority of OSPF routes.	It is an integer ranging from 1 to 255.
route-policy-name	Specifies the routing strategy name.	-

Default Value

None

View

OSPFv2 rouing configuration view

Usage Guidelines

None

Example

Configure the priority of OSPF routes.

```
switch(config-ospf-1)#preference 10
switch(config-ospf-1)#
```

4.4.77 preference ase

Function

The **preference ase** command configures the priority of OSPF external routes.
The **no preference ase** command deletes the priority configuration of the ASE / NSSA route.

Format

- **preference ase** *priority*
- **preference ase** *priority* **route-policy** *route-policy-name*
- **no preference ase**

Parameters

Parameters	Description	Value
priority	Specifies the priority of OSPF external routes.	It is an integer ranging from 1 to 255.
route-policy-name	Specifies the routing strategy name.	-

Default Value

None

View

OSPFv2 rouing configuration view

Usage Guidelines

None

Example

Configure the priority of OSPF external routes.

```
switch(config-ospf-1)#preference ase 100
```

```
switch(config-ospf-1)#
```

4.5 OSPFv3 Configuration Command

4.5.1 area nssa

Function

area nssa command is used to configure a particular area in OSPF as NSSA area.
no area nssa command is used to recover the NSSA area back to normal one.

Format

- **area** *area-id* **nssa**
- **no area** *area-id* **nssa**

Parameters

Parameters	Description	Value
area-id	area ID	Form of IP address dotted decimal or integers. Usually the integer form is for area with ID smaller than 65535 while dotted decimal form is for area with ID larger than 65535, the range is between 0~4294967295

Default Value

No NSSA area

View

OSPFv3 Route Configuration View

Usage Guidelines

The action of NSSA area is similar as Stub area, the difference is that ASSA area is able to send exterior route outwards but not receive route from exterior. Routers in NSSA area will generate Type7 LSA for exterior route, those LSAs in the area will be calculated according to exterior route; ABR will translate the Type7 LSA into Type5 LSA and send it to other areas. The ABR also generates a default Summary LSA for NSSA area.
NSSA area has limits as follows:

- NSSA configuration unavailable in backbone area;
- NSSA configuration unavailable in Stub area;
- NSSA configuration unavailable in virtual link transferring area;

Example

Configure area1 as an NSSA area.

```
switch(config-ospfv3-1)#area 1 nssa
switch(config-ospfv3-1)#
```

4.5.2 area nssa range

Function

area nssa range command is used to configure aggregation route item of NSSA area.
no area nssa range command is used to delete the configured aggregation route item of NSSA area.

Format

- **area** *area-id* **nssa range** *dst-network/dst-mask* { **advertise** | **not-advertise** }
- **no area** *area-id* **nssa range** *dst-address/dst-mask*

Parameters

Parameters	Description	Value
area-id	area ID	Form of IP address dotted decimal or integers. Usually the integer form is for area with ID smaller than 65535 while dotted decimal form is for area with ID larger than 65535, the range is between 0~4294967295
dst-network	aggregation address	-
dst-mask	aggregation mask	-
advertise	receive aggregation item	-
no-advertise	deny aggregation item	-

Default Value

None

View

OSPFV3 Route Configuration View

Usage Guidelines

None

Example

Delete the aggregation route item.

```
switch(config-ospfv3-1)#no area 0 nssa range 2000::1/64
switch(config-ospfv3-1)#
```

4.5.3 area range

Function

area range command is used to configure aggregation route item in a particular area. **no area range** command is used to delete an existing aggregation route item.

Format

- **area** *area-id* **range** *dst-address/dst-mask* { **advertise** | **not-advertise** }
- **no area** *area-id* **range** *dst-address/dst-mask*

Parameters

Parameters	Description	Value
area-id	area ID	Form of IP address dotted decimal or integers. Usually the integer form is for area with ID smaller than 65535 while dotted decimal form is for area with ID larger than 65535, the range is between 0~4294967295
dst-address	aggregation address	-
dst-mask	aggregation mask length	-
advertise	receive aggregation item	-
no-advertise	deny aggregation item	-

Default Value

No include any aggregation item of OSPF area

View

OSPFv3 Route Configuration View

Usage Guidelines

When an ABR calculates route for an area, assuming A, it needs to advertise route information inside the area A to other areas, it generates a Summary LSA to every other area. In this case if the inside route is too large, there will be too many Summary LSAs. Then aggregation item can be provisioned in area A to control the number of Summary LSA.
Once the aggregation item is provisioned, route that matches with the item in area A will not appear in Summary LSAs of other areas. There will two different situations according to differences of advertise attribute in aggregation item:

- advertise' operation is designated and Summary LSA is generated for aggregation item;
- not-advertise' operation is designated and no Summary LSA is generated for aggregation item.

Warning: The command is applied only to existing areas.

Example

The following command enables area1 to include the summray LSA of 2000::1/64 only.

```
switch (config-ospfv3-1)#area 0 range 2000::1/64 advertise
switch(config-ospfv3-1)#
```

The following command enables area1 to exclude the summray LSAs in the range of 2000::1/64.

```
switch(config-ospfv3-1)#area 0 range 2000::1/64 not-advertise
switch(config-ospfv3-1)#
```

4.5.4 area stub

Function

area stub command is used to configure the specific OSPF area as the stub area.
no area stub command is used to cancel the Stub area and recover it back to normal one.

Format

- **area** *area-id* **stub** [**no-summary**]
- **no area** *area-id* **stub**

Parameters

Parameters	Description	Value
area-id	area ID	Form of IP address dotted decimal or integers. Usually the integer form is for area with ID smaller than 65535 while dotted decimal form is for area with ID larger than 65535, the range is between 0~4294967295
[no-summary]	Once the keyword is defined, ABR generates default Summary LSA only for stub area, other area routes will be no Summary LSA generated.	-

Default Value

OSPF area default to be non-stub area

View

OSPFv3 Route Configuration View

Usage Guidelines

The command will designate an area into a Stub area. The Stub area does not contain exterior route (i.e., Type5 LSA) or generate exterior route. The limits of Stub area are as follows:

- Backbone area cannot be deployed as Stub area;
- An area who has been deployed as virtual link transfer area cannot be deployed as Stub area again, otherwise there might be working abnormal;

Once the Stub area is designated, ABR will generate a default Summary LSA for the area with other Summary LSAs' generating as usual. If the no-summary attribute is defined, ABR will clear up other non-default Summary LSA and own one default Summary LSA only.

The objective of designating Stub area is to control LSA number inside the area that if there is limited memory of routers inside the area, huge amount of LSAs cannot be properly received by them, thus Stub area can be defined to solve the problem.

The area that has been designated as Stub is cannot be virtual link transfer area anymore; All routers inside the Stub area must have same Stub attributes otherwise there will be no neighbor established among them.

Example

Restore a Stub area as a common area.

```
switch(config-ospfv3-1)#no area stub
switch(config-ospfv3-1)#
```

4.5.5 area stub no-summary

Function

area stub no-summary command is used to configure the area as no-summary area.

Format

- **area** *area-id* **stub no-summary**

Parameters

Parameters	Description	Value
area-id	area ID	Form of IP address dotted decimal or integers. Usually the integer form is for area with ID smaller than 65535 while dotted decimal form is for area with ID larger than 65535, the range is between 0~4294967295

Default Value

None

View

OSPFv3 Route Configuration View

Usage Guidelines

ABR inside the area is able to not to generate other Summary LSA to Stub area so that to further compress LSA scale, in this case the Stub area can be called as Totally Stub area.

Example

Configure area 1.3.2.1 as a totally Stub area.

```
switch(config-ospfv3-1)#area 1.3.2.1 stub no-summary
switch(config-ospfv3-1)#
```

4.5.6 area nssa no-summary

Function

area nssa no-summary command is used to configure the area as complete NSSA area.

Format

- **area** *area-id* **nssa no-summary**

Parameters

Parameters	Description	Value
area-id	area ID	Form of IP address dotted decimal or integers. Usually the integer form is for area with ID smaller than 65535 while dotted decimal form is for area with ID larger than 65535, the range is between 0~4294967295

Default Value

None

View

OSPFv3 Route Configuration View

Usage Guidelines

None

Example

Configure area 1 as a total NSSA area.

```
switch(config-ospfv3-1)#area 1 nssa no-summary
switch(config-ospfv3-1)#
```

4.5.7 bandwidth-reference

Function

The **bandwidth-reference** command sets the reference for link cost calculation.

Format

- **bandwidth-reference** { *bandwidth* | **default** }

Parameters

Parameters	Description	Value
bandwidth	Specifies the range of reference rate.	It is an integer ranging from 1 to 100000 (unit: Mbit/s)

Default Value

The reference link cost is 100 Mbit/s.

View

OSPFv3 configuration view

Usage Guidelines

None

Example

Set the reference link cost to 1000.

```
switch(config-ospfv3-1)#bandwidth-reference 1000
switch(config-ospfv3-1)
```

4.5.8 graceful-restart

Function

The **graceful-restart** command enables the grace restart.
The **no graceful-restart** command disables the grace restart.

Format

- **graceful-restart**
- **graceful-restart** [**period** *restart-time*]
- **no graceful-restart**

Parameters

Parameters	Description	Value
restart time	Specifies the restarting time.	It is an integer ranging from 40 to 1800 (s).
period	Sets the restarting period.	-

Default Value

None

View

OSPFv3 configuration view

Usage Guidelines

None

Example

Enable the grace restart.

```
switch(config-ospfv3-1)#graceful-restart
switch(config-ospfv3-1)#
```

4.5.9 graceful-restart begin

Function

The **graceful-restart begin** command enables graceful OSPF restart, preventing the routing oscillation caused by traffic interruption or active/standby switch.

Format

- **graceful-restart begin**

Parameters

None

Default Value

None

View

OSPFv3 configuration view

Usage Guidelines

None

Example

Enable the OSPF graceful restart planning.

```
switch(config-ospfv3-1)#graceful-restart begin
switch(config-ospfv3-1)#
```

4.5.10 graceful-restart helper

Function

The **graceful-restart helper** command enables or disables the OSPF graceful restart helper.

Format

- **graceful-restart helper**
- **no graceful-restart helper**

Parameters

None

Default Value

None

View

OSPFv3 configuration view

Usage Guidelines

None

Example

Enable the OSPF graceful restart helper.

```
switch(config-ospfv3-1)#graceful-restart helper
switch(config-ospfv3-1)#
```

4.5.11ipv6 ospf if-type

Function

ipv6 ospf if-type command is used to configure OSPFv3 interface type.

Format

- **ipv6 ospf if-type** { **broadcas** | **p2p** }
- **ipv6 ospf if-type** { **broadcas** | **p2p** } **process** *process-id*

Parameters

Parameters	Description	Value
broadcast	Broadcast interface type, default type	-
p2p	Point to Point interface type	-
process-id	Process number	integer, 1-127

Default Value

Broadcast

View

VLANIF Configuration View, Interface Configuration View(Ethernet)

Usage Guidelines

None

Example

Configure the OSPFv3 interface type to broadcast.

```
switch(config-vlanif-3)#ipv6 ospf if-type broadcast
switch(config-vlanif-3)#
```

4.5.12 ipv6 ospf hello-interval

Function

ipv6 ospf hello-interval command is used to configure the hello interval of IPv6 OSPF interface.
ipv6 ospf hello-interval default command is used to recover the hello interval back to default.

Format

- **ipv6 ospf hello-interval** { *hello-interval* | **default** }
- **ipv6 ospf hello-interval** { *hello-interval* | **default** } **process** *process-id*

Parameters

Parameters	Description	Value
hello-interval	the hello interval of Ipv6 OSPF interface	integer, 1-65535
process-id	OSPFv3 process nubmer	integer, 1-8

Default Value

10

View

VLANIF Configuration View, Interface Configuration View(Ethernet)

Usage Guidelines

Under default situation, the hello-interval of OSPF interface is 10 seconds. The value can be edited but it is noticed that both of the neighbors must have same interval time and the interval must be smaller than 1/3 of dead-interval.

Example

Configure the hello interval of an OSPF interface to 20s.

```
switch(config-vlanif-3)#ipv6 ospf hello-interval 20
switch(config-vlanif-3)#
```

4.5.13 ipv6 ospf dead-interval

Function

ipv6 ospf dead-interval command is used to configure the neighbor timeout of IPv6 OSPF interface.
ipv6 ospf dead-interval default command is used to recover the timeout time back to default.

Format

- **ipv6 ospf dead-interval** { *interval* | **default** }
- **ipv6 ospf dead-interval** { *interval* | **default** } **process** *process-id*

Parameters

Parameters	Description	Value
interval	the neighbor timeout of IPv6 OSPF interface	integer, 1~65535
process-id	OSPFv3 process ID	integer, 1-8

Default Value

The neighbor timeout of IPV4 OSPF interface is 40s.

View

VLANIF Configuration View

Usage Guidelines

The command can be used to set or change default timeout value of OSPF interface neighbor. It is noticed that both of the neighbors must configure same timeout value and the value must be larger than (3* interface hello-interval).

Example

Configure the neighbor timeout of an OSPF interface to 30s.

```
switch(config-vlanif-3)#ipv6 ospf dead-interval 30
switch(config-vlanif-3)#
```

4.5.14 ipv6 ospf transmit-delay

Function

Ipv6 ospf transmit-delay command is used to configure OSPF interface transmitting delay.

Format

- **ipv6 ospf transmit-delay** { *transmit-delay-time* | **default** }
- **ipv6 ospf transmit-delay** { *transmit-delay-time* | **default** } **process** *process-id*

Parameters

Parameters	Description	Value
transmit-delay-time	OSPF interface transmitting delay	integer, 0~65535, unit: second
process-id	OSPFv3 process ID	integer, 1-8

Default Value

1

View

VLANIF Configuration View

Usage Guidelines

OSPF assumes that there is time delay when the interface sends messagesand the default delay is 1 second. The objective to provisioning delay is to implement better control of LSA update. For example, when an LSA with 0 as its Age passes through an interface for transmission, the Age shall be configured as the delay of this interface. However, in terms of the LSA aging time being 3600 seconds that is far larger than real interface transmission delay, that the delay here appears to be less important.
The transmission delay belongs to a local variable and does not need to be synchronized. Both neighbors are able to be configured as different transmission delays.

Example

Set the OSPF interface transmitting delay to 2s.

```
switch(config-vlanif-3)#ipv6 ospf transmit-delay 2
switch(config-vlanif-3)#
```

4.5.15 ipv6 ospf area

Function

ipv6 ospf area command is used to configure the directly connected area information of Switch.

Format

- **ipv6 ospf area** *area-id*
- **ipv6 ospf area** *area-id* **process** *process-id*
- **ipv6 ospf area** *area-id* **process** *process-id* **instance** *instance-id*
- **no ipv6 ospf**
- **no ipv6 ospf process** *process-id*
- **no ipv6 ospf process** *process-id* **instance** *instance-id*

Parameters

Parameters	Description	Value
area-id	area ID	Form of IP address dotted decimal or integers. Usually the integer form is for area with ID smaller than 65535

Parameters	Description	Value
		while dotted decimal form is for area with ID larger than 65535, the range is between 0~4294967295
instance-id	OSPF insatnce ID	integer, 0-255, no configured to be default 0
process-id	OSPFv3 process ID	integer, 1—8

Default Value

None

View

VLANIF Configuration View

Usage Guidelines

None

Example

Configure the directly connected area ID of the Switch to 10000.

```
switch(config-vlanif-1)#ipv6 ospf area 10000
switch(config-vlanif-1)#
```

4.5.16 ipv6 ospf bfd {enable|disable}

Function

ipv6 ospf bfd {enable|disable} command is used to enable or disable BFD feature under VLAN interface.

Format

- **ipv6 ospf bfd** { **enable | disable** }
- **ipv6 ospf bfd** { **enable | disable** } **process** *process-id*

Parameters

Parameters	Description	Value
enable	enable BFD once BFD enabled, OSPF neighbor disconnection can be detected rapidly	-
disable	disable BFD	-
process-id	OSPF process ID	integer, 0-8, no configured to be default 0

Default Value

None

View

VLANIF Configuration View

Usage Guidelines

None

Example

Enable the BFD features.

```
switch(config-vlanif-3)#ipv6 ospf bfd enable
switch(config-vlanif-3)#
```

4.5.17 ipv6 ospf cost

Function

ipv6 ospf cost command is used to configure OSPF interface cost.

Format

- **ipv6 ospf cost** { *cost* | **default** }
- **ipv6 ospf cost** { *cost* | **default** } **process** *process-id*

Parameters

Parameters	Description	Value
cost	cost of running OSPF	integer, 0-65535
default	default automatic setting	-
process-id-id	OSPFv3 process ID	integer, 1-8

Default Value

1

View

VLANIF Configuration View

Usage Guidelines

The OSPF interface cost is used for routing selection control. For example, a gigaethernet port comparing with Ethernet port, the gigaethernet port has higher capacity and can be configured a smaller cost, while on the other hand the Ethernet port can be configured a larger cost. In this case, the gigaethernet port can be selected in higher priority. Generally, There shall be same costs at both sides of neighbor routers.

Example

Set the OSPF interface cost to 20000.

```
switch(config-vlanif-3)#ipv6 ospf cost 20000
switch(config-vlanif-3)#
```

4.5.18 ipv6 ospf peer

Function

ipv6 ospf peer command is used to configure the neighbor Switch IPv6 address and priority in NBMA network.

Format

- **ipv6 ospf peer** *ipv6-address* **priority** *priority*
- **ipv6 ospf peer** *ipv6-address* **priority** *priority* **process** *process-id*

Parameters

Parameters	Description	Value
ipv6-address	neighbor IPV6 address	IP address with 128 bits is separated into 8 groups, 16 bits for each group are represented as 4 hexadecimal strings (0-9, A-F). Groups are separated with colon (:). In those hexadecimals, each 'X' indicates a group of hexadecimal number.
priority	Neighbor priority	integer, 0-255
process-id	OSPFv3 process ID	integer, 1-8

Default Value

None

View

VLANIF Configuration View

Usage Guidelines

None

Example

Set the IPv6 address of the neighbor switch on the OSPF network to 2000::1 and set its priorityto 1.

```
switch(config-vlanif-3)#ipv6 ospf peer 2000::1 priority 1
switch(config-vlanif-3)#
```

4.5.19 ipv6 ospf priority

Function

ipv6 ospf priority command is used to configure OSPF interface priority.

Format

- **ipv6 ospf priority** { *priority* | **default** }
- **ipv6 ospf priority** { *priority* | **default** } **process** *process-id*

Parameters

Parameters	Description	Value
priority	OSPF interface priority	integer, 0-255, unit: byte/second
default	default priority	1
process-id	OSPFv3 process ID	integer, 1-8

Default Value

1

View

VLANIF Configuration View

Usage Guidelines

The OSPF priority is used for interface DR voting that it usually does not need to be provisioned especially when the connection is based on p-2-p mostly, the OSPF interface priority has few usages practically. However, if the administrator expects to have a particular interface played the role of DR, the interface can be recruited with a higher priority. It is noticed that OSPF interface DR cannot be occupied, i.e., once a device being designated as a DR, it will play the role all the time unless it is closed or fault occurs to the device.

Example

Set the OSPF interface priority to 125.

```
switch(config-vlanif-3)#ipv6 ospf priority 125
switch(config-vlanif-3)#
```

4.5.20 ipv6 ospf passive-interface

Function

The **ipv6 ospf passive-interface** command configures the OSPFv3 passive interface.
The **no ipv6 ospf passive-interface** command cancels the OSPFv3 passive interface configuration.

Format

- **ipv6 ospf passive-interface**
- **ipv6 ospf passive-interface process** *process-id*
- **no ipv6 ospf passive-interface**
- **no ipv6 ospf passive-interface process** *process-id*

Parameters

Parameters	Description	Value
process-id	Specifies the OSPFv3 process ID.	It is an integer ranging from 1 to 8.

Default Value

None

View

VLANIF configuration view, Loopback interface configuration view

Usage Guidelines

A passive interface refers to an OSPF interface that does not send or receive protocol messages and does not establish any neighbor relation. However, the interface route is included in the Router LSA for internal route propagation. The passive interface can be used on the Stub routes.

Example

Configure the VLAN3 interface as the OSPF passive interface .

```
switch(config-vlanif-3)#ip ospf passive-interface
switch(config-vlanif-3)#
```

4.5.21 ipv6 ospf retransmit-interval

Function

ipv6 ospf retransmit-interval command is used to configure OSPF interface retransmission interval.

Format

- **ipv6 ospf retransmit-interval** { *retransmit-interval-time* | **default** }
- **ipv6 ospf retransmit-interval** { *retransmit-interval-time* | **default** } **process** *process-id*

Parameters

Parameters	Description	Value
retransmit-interval-time	retransmission interval	integer, 0-1800, unit: second
default	default retransmission interval	5s
process-id	OSPFv3 process ID	integer, 1-8

Default Value

None

View

VLANIF Configuration View

Usage Guidelines

The transmission of OSPF messages utilizes IP encapsulation directly which may cause message lost and the lost messages are required to retransmit. The default retransmit interval is 5 seconds and administrator is able to set the interval according to practical network circumstance.
The retransmit interval belongs to a local variable and it does not need to be synchronized. Neighbors are allowed to provision with different retransmit intervals.

Example

Set the retransmission interval of an OSPF interface to 2s.

```
switch(config-vlanif-3)#ipv6 ospf retransmit-interval 2
switch(config-vlanif-3)#
```

4.5.22 ipv6 ospf mtu

Function

ipv6 ospf mtu command is used to configure interface MTU of OSPF.

Format

- **ipv6 ospf mtu** { *mtu* | **default** }
- **ipv6 ospf mtu** { *mtu* | **default** } **process** *process-id*

Parameters

Parameters	Description	Value
mtu	interface MTU of OSPF	integer, 572-9000
default	interface MTU of OSPF default	1500
process-id	OSPFv3 process ID	integer, 1-8

Default Value

1500

View

VLANIF Configuration View

Usage Guidelines

The default MTU of OSPF interface is IP MTU of interface and if the interface IP MTU is unavailable then the default MTU here will be 0. The command is used to define or change OSPF interface MTU, it shall be noticed that the MTU here is not the IP interface MTU.
Both of neighbors shall have same OSPF interface MTU.

Example

Set the MTU value of an OSPFv3 interface to 1000.

```
switch(config-vlanif-3)#ipv6 ospf mtu 1000
switch(config-vlanif-3)#
```

4.5.23 ipv6 ospf mtu-ignore {enable|disable}

Function

ipv6 ospf mtu-ignore {enable|disable} command is used to enable or disable MTU detection function.

Format

- **ipv6 ospf mtu-ignore** { **enable** | **disable** }
- **ipv6 ospf mtu-ignore** { **enable** | **disable** } **process** *process-id*

Parameters

Parameters	Description	Value
enable	enable MTU detection function.	-
disable	disable MTU detection function.	-
process-id	OSPFv3 process ID	integer, 1-8

Default Value

Disable

View

VLANIF Configuration View, Loopback Interface Configuration View

Usage Guidelines

None

Example

Check the MTU field in the DD packets.

```
switch(config-vlanif-3)#ipv6 ospf mtu-ignore enable
switch(config-vlanif-3)#
```

4.5.24 router ipv6 ospf

Function

router ipv6 ospf command is used to start IPV6 OSPF protocol and access the OSPF configuration view.
no router ipv6 ospf command is used to disable the IPv6 OSPF protocol.

Format

- **router ipv6 ospf**
- **router ipv6 ospf** *process-id*
- **no router ipv6 ospf**
- **no router ipv6 ospf** *process-id*

Parameters

Parameters	Description	Value
process-id	IPv6 OSPF process number	integer, 1-8, default to be 1

Default Value

Disabled

View

Global Configuration View

Usage Guidelines

None

Example

Enable the OSPFv3 protocol.

```
switch(config)#ipv6 router ospf
switch(config-ospfv3-1)#
```

4.5.25 reset ipv6 ospf

Function

reset ipv6 ospf command is used to restart OSPFv3 process.

Format

- **reset ipv6 ospf**
- **reset ipv6 ospf** *process-id*

Parameters

Parameters	Description	Value

Parameters	Description	Value
process-id	OSPFv3 process ID	integer, 1-8

Default Value

None

View

Interface Configuration View, OSPFv3 Route Configuration View

Usage Guidelines

None

Example

Restart the OSPF process.

```
switch(config-ospfv3-1)#reset ipv6 ospf
switch(config-ospfv3-1)#
```

4.5.26 reset ipv6 ospf counters

Function

reset ipv6 ospf counters command is used to clear OSPFv3 counter.

Format

- **reset ipv6 ospf counters**
- **reset ipv6 ospf** *process-id* **counters**

Parameters

Parameters	Description	Value
process-id	OSPFv3 process ID	integer, 1-127

Default Value

None

View

Global Configuration View, OSPFv3 Route Configuration View

Usage Guidelines

None

Example

Clear the OSPFv3 counter.

```
switch(config-ospfv3-1)#reset ipv6 ospf counters
switch(config-ospfv3-1)#
```

4.5.27 redistribute route-policy

Function

The **redistribute route-policy** command configures a route import policy.
The **no redistribute route-policy** command deletes a route import policy.

Format

- **redistribute** { **static** | **connect** | **rip** | **bgp** | **isis** } **route-policy** *policy-name*
- **no redistribute** { **static** | **connect** | **rip** | **bgp** | **isis** }
- **no redistribute** { **static** | **connect** | **rip** | **bgp** | **isis** } **route-policy** *policy-name*

Parameters

Parameters	Description	Usage Guidelines
static	Configures a policy for importing static routes.	Only routes matching specified routing policy can be imported. Name specifies the name of the routing policy for route import. Multiple routing policies can be configured to filter routes imported from other protocols. Multiple routing policies can be configured to filter routes imported from other protocols. Later configured routing policies do not override the previously configured ones. This command takes effect only after static route redistribution is enabled using the redistribute static command.
connect	Configures a policy for importing direct routes.	Only routes matching specified routing policy can be imported. Name specifies the name of the routing policy for route import. Multiple routing policies can be configured to filter routes imported from other protocols. Multiple routing policies can be configured to filter routes imported from other protocols. Later configured routing policies do not override the previously configured ones. This command takes effect only after direct route redistribution is enabled using the

Parameters	Description	Usage Guidelines
		redistribute static command.
rip	Configures route measurement for introducing a RIP route.	Only routes matching specified routing policy can be imported. **Name** specifies the name of the routing policy for route import. Multiple routing policies can be configured to filter routes imported from other protocols. Multiple routing policies can be configured to filter routes imported from other protocols. Later configured routing policies do not override the previously configured ones. This command takes effect only after rip route redistribution is enabled using the redistribute rip bgp command.
bgp	Configures the policy for introducing a BGP route.	Only routes matching specified routing policy can be imported. Name specifies the name of the routing policy for route import. Multiple routing policies can be configured to filter routes imported from other protocols. Multiple routing policies can be configured to filter routes imported from other protocols. Later configured routing policies do not override the previously configured ones. This command takes effect only after BGP route redistribution is enabled using the redistribute bgp command.
isis	Configures the policy for introducing an IS-IS route.	Only routes matching specified routing policy can be imported. Name specifies the name of the routing policy for route import. Multiple routing policies can be configured to filter routes imported from other protocols. Multiple routing policies can be configured to filter routes imported from other protocols. Later configured routing policies do not override the previously configured ones. This command takes effect only after ISIS route redistribution is enabled using the redistribute isis command.
policy-name	Specifies the name of a routing policy.	The value is a string of characters of no more than 20 bytes.

Default Value

The value is a string of blank characters, indicating that no routing policy is referenced.

View

OSPFv3 configuration view

Example

Configure routing policy 2 for importing static routes.

```
switch(config-ospfv3-1)#redistribute static route-policy 2
switch(config-ospfv3-1)#
```

4.5.28 router-id

Function

router-id command is used to configure Switch ID.

Format

- **router-id** *ip-address*

Parameters

Parameters	Description	Value
ipv6-address	Switch ID	-

Default Value

In default, the switch does not have switch ID. A random IP address from switch interfaces will be selected as the switch ID during the operation.

View

OSPFv3 Route Configuration View

Usage Guidelines

The rule of router ID selection is as follows:

- minimum static loopback address;;
- minimum static master address;
- minimum static sub-address;
- minimum static link-local address;
- minimum DHCP designated address;
- error loopback;

Example

Set the router ID to 1.1.1.1.

```
switch(config-ospfv3-1)#router-id 1.1.1.1
switch(config-ospfv3-1)#
```

4.5.29 show ipv6 ospf graceful-restart

Function

show ipv6 ospf graceful-restart command is used to display current graceful restart functionality with its status of OSPF.

Format

- **show ipv6 ospf graceful-restart**
- **show ipv6 ospf graceful-restart process** *process-id*

Parameters

Parameters	Description	Value
process-id	Process number	integer, 1-8

Default Value

None

View

Privilege User View, Global Configuration View, Common User View, OSPFv3 Route Configuration View

Usage Guidelines

None

Example

Check the current graceful restart configuration and status of the OSPF.

```
switch#show ipv6 ospf graceful-restart
 Restart Capability            : Support
Restart Helper Capability     : Support
Restart State                 : Not in Restarting
Restart Period                : 100
Restart Exit Reason       :  completed
Restart Age                   : 50
```

4.5.30 show ipv6 ospf brief

Function

show ipv6 ospf brief command is used to display information of OSPF global Parameters.

Format

- **show ipv6 ospf brief**
- **show ipv6 ospf brief process** *process-id*

Parameters

Parameters	Description	Value
process-id	Process number	integer, 1-8

Default Value

None

View

Privilege User View, Global Configuration View, Common User View, VLANIF Configuration View, kInterface Configuration View(Ethernet)

Usage Guidelines

None

Example

Display the OSPF brief.

```
switch#show ipv6 ospf brief
  Ipv6 OSPF Instance 0
  Vpn Name                        :N/A
  Routing Process ID              :10.18.16.100
  AS scope LSA Number             :0
  Checksum Sum                    :0x0000
  External LSA Number             :0
  Area 0.0.0.0 information
  Stub Area                       :No
  SPF Algorithm Executed Times:2
  LSA Number                      :2
  Checksum Sum                    :0x9293
switch#
```

4.5.31 show ipv6 ospf area

Function

show ipv6 ospf area command is used to display information of areas that are directly connected to the switch.

Format

- **show ipv6 ospf area** [*area-id*]
- **show ipv6 ospf area** [**process** *process-id*]

- **show ipv6 ospf area process** *process-id*

Parameters

Parameters	Description	Value
[area-id]	area ID	Form of IP address dotted decimal or integers. Usually the integer form is for area with ID smaller than 65535 while dotted decimal form is for area with ID larger than 65535, the range is between 0~4294967295
process-id	Process number	integer, 1-8

Default Value

None

View

Privilege User View, Global Configuration View, Common User View, OSPFv3 Route Configuration View, VLANIF Configuration View, Interface Configuration View(Ethernet)

Usage Guidelines

The input of the command is able to check whether the OSPF area is correctly configured so that to process OSPF failure check.

Example

Check all areas directly connected to the switch.

```
switch#show ipv6 ospf area
AreaId          Flag(Hex) RouteUpdates     ABR   ASBR  LSA Count
1               8         1                0     0     0

switch#
```

4.5.32 show ipv6 ospf bfd session

Function

show ipv6 ospf bfd session command is used to display information of neighbor enabled BFD.

Format

- **show ipv6 ospf bfd session**

Parameters

None

Default Value

None

View

Privilege User View, Global Configuration View, Common User View, OSPFv3 Route Configuration View, VLANIF Configuration View, LoopbackInterface Configuration View

Usage Guidelines

None

Example

Check the BFD neighbor information.

```
switch#show ipv6 ospf bfd session
OSPFv3 Process 1
Neighbor : fe80::b8:2      NeighborId : 1.1.1.2
Interface : ge1/0/1      BFDState : up
Min TX : 200    Min RX : 200
Multiplier : 3      BFD Local Dis : 1
LocalIpAdd :fe80::b8:1 RemoteIpAdd : fe80::b8:2
Diagnostic Info : noDiagnostic
```

4.5.33 show ipv6 ospf config

Function

show ipv6 ospf config command is used to display information of OSPF protocol operation.

Format

- **show ipv6 ospf config**

Parameters

None

Default Value

None

View

Privilege User View, Global Configuration View, Common User View, OSPFv3 Route Configuration View, VLANIF Configuration View, Interface Configuration View(Ethernet)

Usage Guidelines

None

Example

Check all the areas directly connected to the switch.

```
switch#show ipv6 ospf config
 !
!IPv6 OSPF Configuration
 ipv6 router ospf
 router-id 2000::1
switch#
```

4.5.34 show ipv6 ospf database

Function

show ipv6 ospf database command is used to display databse information of OSPF.

Format

- **show ipv6 ospf database** [**process** *process-id*]
- **show ipv6 ospf database area** *area-id*
- **show ipv6 ospf database area** *area-id* **process** *process-id*
- **show ipv6 ospf database external** *LS-id advertise-router-id*
- **show ipv6 ospf database link** *LS-id advertise-router-id* **interface vlan** *vlan-id*
- **show ipv6 ospf database link** *LS-id advertise-router-id* **interface loopback** *loopback-id*
- **show ipv6 ospf database process** *process-id*
- **show ipv6 ospf database total count**

Parameters

Parameters	Description	Value
area-id	area ID	Form of IP address dotted decimal or integers. Usually the integer form is for area with ID smaller than 65535 while dotted decimal form is for area with ID larger than 65535, the range is between 0~4294967295
LS-id	LS ID	Dotted decimal
advertise-router-id	advertise router ID	Dotted decimal
process-id	process number	integer, 1-8
vlan-id	VLAN ID	integer, 1-4094
loopback-id	loopback interface number	integer, 1-4

Default Value

None

View

Privilege User View, Global Configuration View, Common User View, OSPFv3 Route Configuration View, VLANIF Configuration View, Interface Configuration View(Ethernet)

Usage Guidelines

The input of the command is able to check whether the OSPF database is correctly configured so that to process OSPF failure check.

Example

View the information of the OSPF database.

```
switch# show ipv6 ospf database
 Database of OSPFv3 Process 1
                Router Link State (Area 0.0.0.0)
 LinkId          ADV Router      Age     Seq#       CheckSum   Len
 0.0.0.0         1.1.1.1         42      0x80000002 0x4fef     40
 0.0.0.0         1.1.1.2         43      0x80000002 0x43fc     40
                Network Link State (Area 0.0.0.0)
 LinkId          ADV Router      Age     Seq#       CheckSum   Len
 0.0.39.17       1.1.1.2         43      0x80000001 0x11d1     32
               Intra Area Prefix Link State (Area 0.0.0.0)
 LinkId          ADV Router      Age     Seq#       CheckSum   Len
 0.0.3.232       1.1.1.2         42      0x80000001 0x1a6c     44


               Link(Type-8) State(interface vlan1 Area 0.0.0.0)
 LinkId          ADV Router      Age     Seq#       CheckSum   Len
 0.0.39.17       1.1.1.1         82      0x80000001 0xf91      76
 0.0.39.17       1.1.1.2         83      0x80000001 0x6155     76
                AS External Link State
 LinkId          ADV Router      Age     Seq#       CheckSum   Len        Prefix
 0.0.0.2         1.1.1.1         73      0x80000001 0x7f0a     36         2013:1100:0:1::/64
switch#
```

4.5.35 show ipv6 ospf database count

Function

The **show ipv6 ospf database count** command displays the quantity of OSPFv3 LSAs.

Format

- **show ipv6 ospf database count**
- **show ipv6 ospf database count process** *process-id*

Parameters

Parameters	Description	Value
process-id	Specifies the process ID.	It is an integer ranging from 1 to 8
string	Specifies the matched characterstring.	The value is a character string.

Default Value

None

View

Priviledge user view, global configuration view, common user view, VLANIF configuration view, OSPFv3 configuration view and interface configuration view (Ethernet)

Usage Guidelines

None

Example

View the quantity of OSPFv3 LSAs.

```
Switch#show ipv6 ospf database count
    Database of OSPF Instance 1
   Extern Route: 2
  Unkown Route: 0
   Areaid   1.1.1.1
   RouteLsa    NetworkLsa    InterPrefix   InterRouter   NssaLsa   IntraLsa   UnKnowLsa
     2           3           4             5           1         5          0
  Areaid  2.2.2.2
   RouteLsa    NetworkLsa    InterPrefix   InterRouter   NssaLsa   IntraLsa   UnKnowLsa
     2           3           4             5           1         5          0

  interface vlan-1
   Link LSA Count: 5
   interface vlan-2
   Link LSA Count: 10

  Virtual interface 2
   Link Lsa Count: 2
   Virtual interface 3
   Link Lsa Count: 5
```

```
Switch#
```

4.5.36 show ipv6 ospf interface

Function

show ipv6 ospf interface command is used to display interface information of OSPF.

Format

- **show ipv6 ospf interface**
- **show ipv6 ospf interface vlan** *vlan-id*
- **show ipv6 ospf interface loopback** *loopback-id*
- **show ipv6 ospf interface count**
- **show ipv6 ospf interface process** *process-id*

Parameters

Parameters	Description	Value
process-id	Process number	integer, 1-8
loopback-id	Loopback interface number	integer, 1-4
vlan-id	Specifies the VLAN ID.	integer, 1-4094
string	Specifies the matched character string.	The value is a character string.

Default Value

None

View

Privilege User View, Global Configuration View, Common User View, OSPFv3 Route Configuration View, VLANIF Configuration View, Interface Configuration View (Ethernet)

Usage Guidelines

The input of the command is able to check whether the OSPF interface is correctly configured so that to process OSPF failure check.

Example

View interface table information of OSPF.

```
Switch#show ipv6 ospf interface
OSPF Process 1
 Interface        IpAddr          AreaId          State           Cost
 vlan 14          2000::1          0               down             1
 OSPF Process 2
 Interface        IpAddr          AreaId          State           Cost
```

```
vlan 10          2000::1          0          designatedRouter        1
Switch#
```

4.5.37 show ipv6 ospf neighbor

Function

show ipv6 ospf neighbor command is used to display Switch neighbor information.

Format

- **show ipv6 ospf neighbor** [**process** *process-id*]
- **show ipv6 ospf neighbor** [*ip-address*]
- **show ipv6 ospf neighbor process** *process-id*
- **show ipv6 ospf neighbor state statistic**

Parameters

Parameters	Description	Value
[ip-address]	neighbor IP address, optional Parameters	Dotted decimal
process-id	process number	integer, 1-8
string	Specifies the matched character string.	The value is a character string.

Default Value

None

View

Privilege User View, Global Configuration View, Common User View, OSPFv3 Route Configuration View, VLANIF Configuration View, Interface Configuration View(Ethernet)

Usage Guidelines

The input of the command is able to check whether the OSPF neighbor is correctly configured so that to process OSPF failure check.

Example

View the switch neighbor information.

```
Switch#show ipv6 ospf neighbors
OSPF Process 1
 IpAddress        NeighborID       Priority  State      Aging   UpTime   Interface
2000::10          3000::1          1         full       36      0:01:01  vlan 10
Switch#
```

4.5.38 show ipv6 ospf route

Function

show ipv6 ospf route command is used to display OSPF routing information.

Format

- **show ipv6 ospf route**
- **show ipv6 ospf route process** *process-id*

Parameters

Parameters	Description	Value
process	process number	integer, 1-8
string	Specifies the matched character string.	The value is a character string.

Default Value

None

View

Privilege User View, Global Configuration View, Common User View, OSPFv3 Route Configuration View, VLANIF Configuration View, Interface Configuration View(Ethernet)

Usage Guidelines

None

Example

View the OSPF routing information.

```
Switch#show ipv6 ospf route
 Total 0 routes,Max SPF running time:0ticks
 Number of route search loop:0times,last SPF running time:0ticks
 ABR:0,ASBR:0,Network:0,External:0,Virtual:0
 Last Dijikstra time:0ticks
 Last Summary Calculate time:0ticks
 Last External Calculate time:0ticks
 Last Routing Table Update time:0ticks
Dst                Mask                Nexthop             Type
```

4.5.39 show ipv6 ospf route count

Function

show ipv6 ospf route count command is used to display OSPF routing counter information.

Format

- **show ipv6 ospf route count**
- **show ipv6 ospf route count process** *process-id*
- **show ipv6 ospf route total count**

Parameters

Parameters	Description	Value
process-id	process number	integer, 1-8

Default Value

None

View

Privilege User View, Global Configuration View, Common User View, OSPFv3 Route Configuration View, VLANIF Configuration View, Interface Configuration View(Ethernet)

Usage Guidelines

None

Example

View the OSPF routing counter information.

```
Switch#show ipv6 ospf route count
 Ospfv3 Process 1
 ------------------------------------------------------------------------
 Route :
 Prefix(Intra   Inter   External)   ABR          ASBR
 0        0        0        0             0            0

 Path :
 Prefix(Intra   Inter   External)   ABR          ASBR
 0        0        0        0             0            0

Switch#
```

4.5.40 show ipv6 ospf trap

Function

show ipv6 ospf trap command is used to display the trap information of current configuration.

Format

- **show ipv6 ospf trap**
- **show ipv6 ospf trap process** *process-id*

Parameters

Parameters	Description	Value
process-id	process number	integer, 1-8

Default Value

None

View

Privilege User View, Global Configuration View, Common User View, OSPFv3 Route Configuration View, VLANIF Configuration View, Loopback Interface Configuration View

Usage Guidelines

None

Example

View the trap of the current configuration.

```
switch#show ipv6 ospf trap
 ------------------------------------------------------------
 OSPFv3 Process 1
 Trap number : 12
 ------------------------------------------------------------
 Trap name                          Status      Excessive Flag
 virtifstatechange                   off          N
 nbrstatechange                      off          N
 virtnbrstatechange                  off          N
 ifconfigerror                       off          Y
 virtifconfigerror                   off          Y
 ifrxbadpacket                       off          N
 virtifrxbadpacket                   off          N
 ifstatechange                       off          N
 nssatranslatorstatuschange          off          N
 restartstatuschange                 off          N
 nbrrestarthelperstatuschange        off          N
 virtnbrrestarthelperstatuschange    off          N
switch#
```

4.5.41 filter route-policy

Function

The **filter route-policy** command configures a filter policy of the routing protocol. Only the filtered route is added to the update packet for advertisement.
The **no filter route-policy** command cancels the routing protocol filter policy.

Format

- **filter route-policy** *route-policy-name*
- **no filter route-policy** *route-policy-name*

Parameters

Parameters	Description	Value
route-policy-name	Specifies a routing policy name, which must be configured in the routing policy.	It is a character string.

Default Value

By default, the value is a string of blank characters, indicating that no routing policy is referenced.

View

OSPFv3 configuration view

Usage Guidelines

You can use this command to set the filter criteria for routing information. Only filtered information can be distributed.

Example

Configure filter policy fs1 for the routing protocol.

```
switch(config-ospfv3-1)#filter route-policy fs1
switch (config-ospfv3-1)#
```

4.5.42 spf-running-interval

Function

The **spf-running-interval** command configures the interval of routing calculation.

Format

- **spf-running-interval** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	Specifies the interval of routing calculation.	It is an integer ranging from 1 to 60 (unit: ms).
default	Uses the default interval of routing calculation.	2

Default Value

2

View

OSPFv3 configuration view

Usage Guidelines

None

Example

Configure the interval of routing calculation to 30.

```
switch(config-ospfv3-1)#spf-running-interval 30
switch(config-ospfv3-1)#
```

4.5.43 area nssa translator

Function

The **area nssa translator** command configures a specified transition router or candidate transition router for the ABR in the NSSA area.

Format

- **area** *area-id* **nssa translator** { **always** | **candidate** }

Parameters

Parameters	Description	Value
area-id	Specifies an area ID.	The value is a dotted decimal number (same as the IPv6 address) or an integer. Generally, for an area with ID smaller than 65535, the value is an integer. For an area with ID larger than 65535, the value is an IPv6 address. The value ranges from 0 to 4294967295.
always	Specifies a transition router for the ABR in the NSSA area. Multiple ABRs in the NSSA area can be configured as transition routers.	-
candidate	Specifies a candidate transition	-

Parameters	Description	Value
	router for the ABR in the NSSA area. If no conversion router is designated in the current area, the conversion router is elected from all the candidate routers.	

Default Value

None

View

OSPFV3 CONFIGURATION VIEW

Usage Guidelines

None

Example

Specify a transition router for the ABR in the NSSA area.

```
switch(config-ospfv3-1)#area 1000 nssa translator always
switch(config-ospfv3-1)#
```

4.6 BGP Configuration Commands

4.6.1 ipv4[ipv6]-family

Function

The **ipv4[ipv6]-family** command enters address family views of BGP.

Format

- **ipv4-family unicast**
- **ipv6-family unicast**

Parameters

Parameter	Description	Value
unicast	Enters the unicast address family view.	-

Default Value

None

View

BGP configuration view

Usage Guidelines

If this parameter is not specified, the unicast address family view is displayed by default.

Example

Enter the unicast address family view of BGP.

```
switch(config-bgp)#ipv4-family unicast
switch(config-bgp-af-ipv4)#
```

Related Commands

None

4.6.2 aggregate

Function

The **aggregate** command creates an aggregation record in the BGP routing table.
The **no aggregate** command deletes a corresponding record.

Format

- **aggregate** *ipv4-address ipv4-mask-length* { **summaryonly** | **all** }
- **aggregate** *ipv6-address ipv6-mask-length* { **summaryonly** | **all** }
- **no aggregate** *ipv4-address ipv4-mask-length*
- **no aggregate** *ipv6-address ipv6-mask-length*

Parameters

Parameter	Description	Value
ipv4-address	Specifies an aggregate IPv4 address.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.
ipv6-address	Specifies an aggregate IPv6 address.	The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.
ipv4-mask-length	Specifies the mask length of an IPv4 address.	The value is an integer ranging from 0 to 32.
ipv6-mask-length	Specifies the mask length of an IPv6 address.	The value is an integer ranging from 0 to 128.
summaryonly | all	Specifies whether to send only an aggregate route, or both an aggregate route and a specific route.	-

Default Value

None

View

BGP configuration view, address family configuration view

Usage Guidelines

When aggregating the addresses of a certain network segment, you can use this command to reduce the number of routing entries transmitted on the network.

Example

Create an aggregation record with address 10.10.10.10 10 in the BGP routing table.

```
switch(config-bgp)#aggregate 10.10.10.10 10 summaryonly
switch(config-bgp)#
```

Related Commands

None

4.6.3 aggregate adminstatus

Function

The **aggregate adminstatus** command validates or invalidates an aggregation entry.

Format

- **aggregate** *ipv4-address ipv4-mask-length* **adminstatus** { **up** | **down** }
- **aggregate** *ipv6-address ipv6-mask-length* **adminstatus** { **up** | **down** }

Parameters

Parameter	Description	Value
ipv4-address	Specifies an aggregate IPv4 address.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.
ipv6-address	Specifies an aggregate IPv6 address.	The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.
ipv4-mask-length	Specifies the mask length of an IPv4 address.	The value is an integer ranging from 0 to 32.
ipv6-mask-length	Specifies the mask length of an IPv6 address.	The value is an integer ranging from 0 to 128.
up | down	Validates or invalidates an aggregation entry.	-

Default Value

None

View

BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Validate an aggregation entry.

```
switch(config-bgp)#aggregate 10.10.10.10 10 adminstatus up
switch(config-bgp)#
```

Related Commands

None

4.6.4 confederation identifier

Function

The **confederation identifier** command configures a confederation ID.
The **no confederation identifier** command cancels a confederation ID.

Format

- **confederation identifier** *autonomy-system-number*
- **no confederation identifier**

Parameters

Parameter	Description	Value
autonomy-system-number	Specifies the AS number of a confederation.	The value is an integer ranging from 1 to 65535.

Default Value

None

View

BGP configuration view

Usage Guidelines

Similar to the reflection function, the BGP confederation function is used to reduce connections within the BGP autonomous system. It allows you to divide a large autonomous system into several small autonomous systems, but the entire confederation is equivalent to an autonomous system for the external autonomous systems. You can use this command to configure the AS number of a BGP confederation.

Example

Configure a confederation ID.

```
switch(config-bgp)#confederation identifier 1000
switch(config-bgp)#
switch(config-bgp)#no confederation identifier
switch(config-bgp)#
```

Related Commands

None

4.6.5 confederation peer-as

Function

The **confederation peer-as** command specifies the AS numbers belonging to one confederation.
The **no confederation peer-as** command cancels the configuration.

Format

- **confederation peer-as** *autonomy-system-number*
- **no confederation peer-as** *autonomy-system-number*

Parameters

Parameter	Description	Value
autonomy-system-number	Specifies the unique AS number of a small autonomous system in a confederation.	The value is an integer ranging from 1 to 65535.

Default Value

None

View

BGP configuration view

Usage Guidelines

None

Example

Specify the AS numbers belonging to one confederation.

```
switch(config-bgp)#confederation peer-as 1000
switch(config-bgp)#
switch(config-bgp)#no bgp confederation peers 1000
switch(config-bgp)#
```

Related Commands

None

4.6.6 cluster-id

Function

The **cluster-id** command configures a route reflector cluster ID.
The **no cluster-id** command cancels a route reflector cluster ID.

Format

- **cluster-id** *router-id*
- **no cluster-id**

Parameters

Parameter	Description	Value
router-id	Specifies a cluster ID.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.

Default Value

None

View

BGP configuration view

Usage Guidelines

None

Example

Configure a route reflector cluster ID.

```
switch(config-bgp)#cluster-id 20.20.20.20
switch(config-bgp)#
switch(config-bgp)#no cluster-id
switch(config-bgp)#
```

Related Commands

None

4.6.7 community

Function

The **community** command sets a community attribute value to be sent to a peer.
The **no community** command cancels the community attribute setting.

Format

- **community** { *community-value* | **noadvertise** | **noexport** } { **additive** | **replace** | **none** }
- **no community**

Parameters

Parameter	Description	Value
community-value	Specifies the community attribute value.	The value is an integer ranging from 0 to 4294967295.
noadvertise | noexport	Specifies the two most commonly used community values, which are set to 0xffffff01 and 0xffffff02. When the community value in a received route update message is noadvertise, the route is no longer sent to other peers. When the value is noexport, the route is no longer sent to external peers.	-
additive | replace | none	Specifies the ways to send the community attribute to the peer. additive is to add the attribute setting to the end of the original attribute. replace is to send only the attribute setting. none is not to send the community attribute.	-

Default Value

None

View

BGP configuration view

Usage Guidelines

You can use this command to control route advertisement by controlling the community attribute.

Example

Set a community attribute value to be sent to a peer.

```
switch(config-bgp)#community 2000 additive
switch(config-bgp)#
switch(config-bgp)#no community
switch(config-bgp)#
```

Related Commands

None

4.6.8 dampening

Function

The **dampening** command configures the route oscillation dampening suppression parameter of BGP.

Format

- **dampening** { *value1* | **default** } { *value2* | **default** } { *value3* | **default** } { *value4* | **default** }

Parameters

Parameter	Description	Value
value1	Specifies the half-life for dampening.	The value is an integer ranging from 1 to 45, minutes.
default	Specifies the default half-life for dampening.	The default value is 15 minutes.
value2	Specifies the threshold for exiting the suppression state.	The value is an integer ranging from 1 to 20000.
default	Specifies the default threshold for exiting the suppression state.	750
value3	Specifies the threshold for entering the suppression state.	The value is an integer ranging from 1 to 20000.
default	Specifies the default threshold for entering the suppression state.	2000
value4	Specifies the upper limit for dampening.	The value is an integer ranging from 1001 to 20000.
default	Specifies the default upper limit for dampening.	16000

Default Value

The default values of the previous four parameters are 15, 750, 2000, and 16000.

View

BGP configuration view

Usage Guidelines

You can use this command to configure the route oscillation dampening suppression parameter of BGP. The parameter takes effect only when oscillation dampening suppression is enabled. Generally, it does not need to be modified.

Example

Configure the route oscillation dampening suppression parameter of BGP.

```
switch(config-bgp)#dampening 1 100 234 10000
switch(config-bgp)#
```

Related Commands

None

4.6.9 debug bgp

Function

The **debug bgp**command enables BGP debugging.
The **no debug bgp** command disables BGP debugging.

Format

Privileged user view, BGP configuration view

- **debug bgp**
- **no debug bgp**
- **debug bgp** { **update** | **rib-tree** | **route** | **event** | **tcp** | **packet** | **all** | **orf** | **graceful-restart** | **error** | **sync** }
- **no debug bgp** { **update** | **rib-tree** | **route** | **event** | **tcp** | **packet** | **all** | **orf** | **graceful-restart** | **error** | **sync** }

BGP configuration view, IPv4 address family configuration view

- **debug bgp neighbor** *ipv4-address*
- **no debug bgp neighbor** *ipv4-address*

BGP configuration view, IPv6 address family configuration view

- **debug bgp neighbor** *ipv6-address*
- **no debug bgp neighbor** *ipv6-address*

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of the VLANIF interface.	The value is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of the VLANIF interface.	A 128-bit IPv6 address is divided into 8 groups, with 16 bits in each group. Each group is expressed by four hexadecimal digits (0-9 and A-F), and two groups are separated with a colon (:). Each X represents a group of hexadecimal digits.

Default Value

By default, BGP debugging is disabled.

View

Privileged user view, BGP configuration view, IPv4 address family configuration view, IPv6 address family configuration view

Usage Guidelines

None

Example

Enable BGP debugging.

```
switch#debug bgp update
switch#
```

Related Commands

None

4.6.10 default local-med

Function

The **default local-med** command configures the default local MED value of BGP.

Format

- **default local-med** { *local-med* | **default** }

Parameters

Parameter	Description	Value
local-med	Specifies the attribute value.	The value is an integer ranging from 1 to 20000.
default	Specifies the default attribute value of local-preference.	100

Default Value

100

View

BGP configuration view

Usage Guidelines

None

Example

Configure the default local MED value of BGP.

```
switch(config-bgp)#default local-med 200
switch(config-bgp)#
```

Related Commands

None

4.6.11default local-preference

Function

The **default local-preference** command configures the default local preference attribute value of BGP.

Format

- **default local-preference** { *preference-value* | **default** }

Parameters

Parameter	Description	Value
preference-value	Specifies the attribute value.	The value is an integer ranging from 1 to 4294967295.
default	Specifies the default attribute value of local-preference.	100

Default Value

100

View

BGP configuration view

Usage Guidelines

None

Example

Configure the default local preference attribute value of BGP.

```
switch(config-bgp)#default local-preference 100
switch(config-bgp)#
```

Related Commands

None

4.6.12 filter-policy {export|import} route-policy

Function

The **filter-policy {export|import} route-policy** command configures the route filtering policy.
The **no filter-policy {export|import} route-policy** command cancels the configuration.

Format

- **filter-policy** { **export** | **import** } **route-policy** *route-policy-name*
- **no filter-policy** { **export** | **import** } **route-policy** *route-policy-name*

Parameters

Parameter	Description	Value
export | import	Route update information applied to advertisement or learning	-
route-policy-name	Specifies the name of a routing policy.	-

Default Value

None

View

BGP configuration view, BGP-IPv4 unicast/multicast address family view, BGP-IPv6 unicast address family view

Usage Guidelines

After a protocol is configured, the command only filters the specified protocol. After a routing policy is configured, the filtered routing entries must also conform to the routing policy configuration.

Example

Configure a route filtering policy.

```
switch(config-bgp)#filter-policy export route-policy fs
switch(config-bgp)#
```

Related Commands

None

4.6.13 filter-policy export

Function

The **filter-policy** command configures a route filtering policy.
The **no filter-policy** command cancels the configuration.

Format

- **filter-policy export** { **static** | **connected** | **rip** | **ospf** | **isis** } **route-policy** *route-policy-name*
- **no filter-policy export** { **static** | **connected** | **rip** | **ospf** | **isis** } **route-policy** *route-policy-name*

Parameters

Parameter	Description	Value
static | connected | rip | ospf	Specifies the static, direct connect, RIP, and OSPF routes.	-
route-policy-name	Specifies the name of a routing policy.	-

Default Value

None

View

BGP configuration view, BGP-IPv4 unicast/multicast address family view, BGP-IPv6 unicast address family view

Usage Guidelines

After a protocol is configured, the command only filters the specified protocol. After a routing policy is configured, the filtered routing entries must also conform to the routing policy configuration.

Example

Configure a route filtering policy.

```
switch(config-bgp)#filter-policy export route-policy fs
switch(config-bgp)#
```

Related Commands

None

4.6.14 graceful-restart timer restart

Function

The **graceful-restart timer restart** command configures the maximum wait time from discovering local restart by a peer to re-establishing a BGP session.

Format

- **graceful-restart timer restart** { *restart-time* | **default** }

Parameters

Parameter	Description	Value
restart-time	Specifies the wait time.	The value is an integer ranging from 3 to 600, in seconds.
default	Specifies the default wait time.	The default value is 90s.

Default Value

The default value is 90s.

View

BGP configuration view

Usage Guidelines

None

Example

Configure the maximum wait time from discovering local restart by a peer to re-establishing a BGP session.

```
switch(config-bgp)#graceful-restart timer restart 100
switch(config-bgp)#
```

Related Commands

None

4.6.15 graceful-restart timer selection-deferral

Function

The **graceful-restart timer selection-deferral** command configures the deferral route selection time for graceful restart.

Format

- **graceful-restart timer selection-deferral** { *select-time* | **default** }

Parameters

Parameter	Description	Value
select-time	Specifies the selection wait time.	The value is an integer ranging from 3 to 3000, in seconds.

Default Value

The default value is 600s.

View

BGP configuration view

Usage Guidelines

None

Example

Configure the deferral route selection time for graceful restart.

```
switch(config-bgp)#graceful-restart timer selection-deferral 300
switch(config-bgp)#
```

Related Commands

None

4.6.16 maximum load-balancing

Function

The **maximum load-balancing** command sets the maximum number of equal-cost routes for load balancing.

Format

- **maximum load-balancing** { *load-balancing-number* | **default** }

Parameters

Parameter	Description	Value
load-balancing-number	Specifies the maximum number of equal-cost routes for load balancing.	The value is an integer ranging from 1 to 8.
default	Specifies the default maximum number of equal-cost routes for load balancing.	1

Default Value

1

View

BGP configuration view

Usage Guidelines

None

Example

Set the maximum number of equal-cost routes for load balancing.

```
switch(config-bgp)#maximum load-balancing 2
switch(config-bgp)#
```

Related Commands

None

4.6.17 network

Function

The **network** configures the local network routes advertised by BGP, that is, statically add the routes in the local routing table to the BGP routing table and advertise them to the peers.
The **no network** command deletes existing configuration.

Format

- **network** *network-address network-mask*
- **no network** *network-ipv4-address network-mask*
- **no network** *network-ipv6-address/mask-length*

Parameters

Parameter	Description	Value
network-address network-ipv4-address network-ipv6-address	Specifies the IPv4 or IPv6 addresses advertised by BGP.	-
network-mask	Specifies the IPv4 subnet mask.	The value is an IP address mask. If no mask is specified, it is treated as a classful address.
mask-length	Specifies the IPv6 mask length.	The value is an integer ranging from 0 to 128.

Default Value

None

View

BGP configuration view, BGP-IPv4 unicast/multicast address family view, BGP-IPv6 unicast address family view

Usage Guidelines

None

Example

Configure the local network routes advertised by BGP.

```
switch(config-bgp-af-ipv4)#network 10.18.2.105 255.255.255.0
switch(config-bgp-af-ipv4)#
```

Related Commands

None

4.6.18 neighbor

Function

The **neighbor** command enables or disables routing information exchange with a specified peer.

Format

- **neighbor** *ipv4-address* { **enable** | **disable** }
- **neighbor** *ipv6-address* { **enable** | **disable** }
- **no neighbor** *ipv4-address*

- **no neighbor** *ipv6-address*

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a neighbor.	The value is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a neighbor.	A 128-bit IPv6 address is divided into 8 groups, with 16 bits in each group. Each group is expressed by four hexadecimal digits (0-9 and A-F), and two groups are separated with a colon (:). Each X represents a group of hexadecimal digits.

Default Value

By default, ECMP load balancing is disabled.

View

BGP configuration view, BGP-IPv4 unicast/multicast address family view, BGP-IPv6 unicast address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view

Usage Guidelines

If you enable or disable a BGP peer in an address family, for example, run **neighbor enable** or **neighbor disable** in the VPNv4 address family, the BGP connections of the peer in other address families will be interrupted for automatic re-negotiation.

Example

Enable routing information exchange with a specified peer.

```
switch(config-bgp)#neighbor 1.1.1.1 enable
switch(config-bgp)#
```

Related Commands

None

4.6.19 neighbor advertisement-interval

Function

The **neighbor advertisement-interval** command configures the minimum time interval for generating route update packets by BGP.

Format

- **neighbor** *ipv4-address* **advertisement-interval** { *time-interval* | **default** }
- **neighbor** *ipv6-address* **advertisement-interval** { *time-interval* | **default** }

Parameters

Parameter	Description	Value
ipv4-address	IPv4 address of the neighbor	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.
ipv6-address	Specifies the IPv6 address of a neighbor.	The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.
time-interval default	Specifies the timer interval. Specifies the default value.	The value is an integer ranging from 1 to 255. 30

Default Value

30

View

BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Configure the minimum time interval for generating route update packets by BGP.

```
switch(config-bgp)#neighbor 1.1.1.1 advertisement-interval 100
switch(config-bgp)#
```

Related Commands

None

4.6.20 neighbor as-origin-interval

Function

The **neighbor as-origin-interval** command configures the minimum time interval for generating BGP route update packets by BGP.

Format

- **neighbor** *ipv4-address* **as-origin-interval** { *origin-interval* | **default** }
- **neighbor** *ipv6-address* **as-origin-interval** { *origin-interval* | **default** }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.
ipv6-address	Specifies the IPv6 address of a neighbor.	The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.
origin-interval	Specifies the time interval.	The value is an integer ranging from 1 to 65535.
default	Specifies the default time interval.	15

Default Value

None

View

BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Configure the minimum time interval for generating BGP route update packets by BGP.

```
switch(config-bgp)#neighbor 1.1.1.1 as-origin-interval 100
switch(config-bgp)#
```

Related Commands

None

4.6.21 neighbor connect-retry-interval

Function

The **neighbor connect-retry-interval** command configures the time interval for initiating reconnection to a peer after disconnection.

Format

- **neighbor** *ipv4-address* **connect-retry-interval** { *retry-interval* | **default** }
- **neighbor** *ipv6-address* **connect-retry-interval** { *retry-interval* | **default** }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.
ipv6-address	Specifies the IPv6 address of a neighbor.	The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.
retry-interval	Specifies the time interval.	The value is an integer ranging from 1 to 65535.
default	Specifies the default time interval.	20

Default Value

None

View

BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Configure the time interval for initiating reconnection to a peer after disconnection.

```
switch(config-bgp)#neighbor 1.1.1.1 connect-retry-interval 100
switch(config-bgp)#
```

Related Commands

None

4.6.22 neighbor ebgp-multihop

Function

The **neighbor ebgp** command configures BGP neighbors to support multi-hop EBGP.
The **no neighbor ebgp** command cancels the configuration.

Format

- **neighbor** *ipv4-address* **ebgp-multihop**
- **no neighbor** *ipv4-address* **ebgp-multihop**
- **neighbor** *ipv6-address* **ebgp-multihop**
- **no neighbor** *ipv6-address* **ebgp-multihop**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.
ipv6-address	Specifies the IPv6 address of a neighbor.	The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.

Default Value

None

View

BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Configure BGP neighbors to support multi-hop EBGP

```
switch(config-bgp)#neighbor 1.1.1.1 ebgp-multihop
switch(config-bgp)#
```

Related Commands

None

4.6.23 neighbor keepalive-timer hold-timer

Function

The **neighbor keepalive-timer hold-timer** command configures the keepalive time and hold time between peers.

Format

- **neighbor** *ipv4-address* **keepalive-timer** { *keep-value* | **default** } **hold-timer** { *hold-value* | **default** }
- **neighbor** *ipv6-address* **keepalive-timer** { *keep-value* | **default** } **hold-timer** { *hold-value* | **default** }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.
ipv6-address	Specifies the IPv6 address of a neighbor.	The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.

Parameter	Description	Value
keep-value	Specifies the keepalive time.	The value is an integer ranging from 1 to 21845, in seconds. The default value is 30.
hold-value	Specifies the hold time.	The value is an integer ranging from 3 to 65535, in seconds. The default value is 90.

Default Value

None

View

BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Configure the keepalive time and hold time between peers.

```
switch(config-bgp)#neighbor 1.1.1.1 keepalive-timer 100 hold-timer 1000
switch(config-bgp)#
```

Related Commands

None

4.6.24 neighbor next-hop-local

Function

The **neighbor next-hop-local** command sets a next-hop value.
The **no neighbor next-hop-local** command cancels the setting.

Format

- **neighbor** *ipv4-address* **next-hop-local**
- **no neighbor** *ipv4-address* **next-hop-local**
- **neighbor** *ipv6-address* **next-hop-local**
- **no neighbor** *ipv6-address* **next-hop-local**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.
ipv6-address	Specifies the IPv6 address of a neighbor.	A 128-bit IPv6 address is divided into 8 groups, with 16 bits in each group. Each group is

Parameter	Description	Value
		expressed by four hexadecimal digits (0-9 and A-F), and two groups are separated with a colon (:). Each X represents a group of hexadecimal digits.

Default Value

None

View

BGP configuration view

Usage Guidelines

None

Example

Set a next-hop value.

```
switch(config-bgp)#neighbor 10.18.2.111 next-hop-local
switch(config-bgp)#
switch(config-bgp)#no neighbor next-hop-local
switch(config-bgp)#
```

Related Commands

None

4.6.25 neighbor route-policy {export|import}

Function

The **neighbor route-policy {export|import}** command specifies a routing policy for routes originating from peers or routes advertised to peers.
The **no neighbor route-policy {export|import}** command cancels the configuration.

Format

- **neighbor** *ipv4-address* **route-policy** *route-policy-name* { **export** | **import** }
- **neighbor** *ipv6-address* **route-policy** *route-policy-name* { **export** | **import** }
- **no neighbor** *ipv4-address* **route-policy** *route-policy-name* { **export** | **import** }
- **no neighbor** *ipv6-address* **route-policy** *route-policy-name* { **export** | **import** }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in

Parameter	Description	Value
		which A to D are decimal numbers ranging from 0 to 255.
ipv6-address	Specifies the IPv6 address of a neighbor.	The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.
export | import	Route update information applied to advertisement or learning	-
route-policy-name	Specifies the name of a routing policy.	-

Default Value

None

View

BGP-IPv4 unicast address family view, BGP-IPv6 unicast address family view.

Usage Guidelines

None

Example

Specify a routing policy for routes originating from peers or routes advertised to peers.

```
switch(config-bgp)#neighbor 1.2.3.1 route-policy rfs1 export
switch(config-bgp)#
```

Related Commands

None

4.6.26 neighbor password

Function

The **neighbor password** command enables MD5 authentication on TCP connections between BGP peers and BGP messages. The **no neighbor password** command cancels the function.

Format

- **neighbor** *ipv4-address* **password** { **cipher** | **plain** } *password*
- **neighbor** *ipv4-address* **password** *password*
- **no neighbor** *ipv4-address* **password**
- **neighbor** *ipv6-address* **password** *password*
- **neighbor** *ipv6-address* **password** { **cipher** | **plain** } *password*
- **no neighbor** *ipv6-address* **password**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.
ipv6-address	Specifies the IPv6 address of a neighbor.	The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.
password	Specifies a plaintext password string.	The value is a string of 1 to 80 characters, without spaces.

Default Value

None

View

BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Enable MD5 authentication on TCP connections between BGP peers and BGP messages.

```
switch(config-bgp)#neighbor 1.1.1.1 password 12345
switch(config-bgp)#
```

Related Commands

None

4.6.27 neighbor remote-as

Function

The **neighbor remote-as** command configures the remote AS number of a peer.
The **no neighbor remote-as** command cancels the remote AS number of a peer.

Format

- **neighbor** *ipv4-address* **remote-as** *as-value*
- **neighbor** *ipv6-address* **remote-as** *as-value*
- **no neighbor** *ipv4-address*
- **no neighbor** *ipv6-address*

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.
ipv6-address	Specifies the IPv6 address of a neighbor.	The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.
as-value	Specifies an AS number.	The value is an integer ranging from 1 to 65535.

Default Value

None

View

BGP configuration view, address family configuration view

Usage Guidelines

None

Note: Before configuring BGP neighbor commands, you must set the remote as parameter to specify the neighbor AS number.

Example

Configure the remote AS number of a peer.

```
switch(config-bgp)#neighbor 1.1.1.1 remote-as 100
switch(config-bgp)#
```

Related Commands

None

4.6.28 neighbor restart

Function

The **neighbor restart** command restarts the BGP neighbor.

Format

- **neighbor** *ipv4-address* **restart**
- **neighbor** *ipv6-address* **restart**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal

Parameter	Description	Value
		numbers ranging from 0 to 255.
ipv6-address	Specifies the IPv6 address of a neighbor.	The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.

Default Value

None

View

BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Restart the BGP neighbor.

```
switch(config-bgp)#neighbor 1.1.1.1 restart
switch(config-bgp)#
```

Related Commands

None

4.6.29 neighbor route-reflector-client

Function

The **neighbor route-reflector-client** command configures an internal BGP peer as a route reflector client and a local party as a route reflector.
The **no neighbor route-reflector-client** command cancels the configuration.

Format

- **neighbor** *ipv4-address* **route-reflector-client**
- **no neighbor** *ipv4-address* **route-reflector-client**
- **neighbor** *ipv6-address* **route-reflector-client**
- **no neighbor** *ipv6-address* **route-reflector-client**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.
ipv6-address	Specifies the IPv6	The IPv6 address contains 128 bits, indicated by

Parameter	Description	Value
	address of a neighbor.	16-bit hexadecimal numbers separated by colons.

Default Value

None

View

BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Configure an internal BGP peer as a route reflector client and a local party as a route reflector.

```
switch(config-bgp)#neighbor 1.1.1.1 route-reflector-client
switch(config-bgp)#
```

Related Commands

None

4.6.30 neighbor route-refresh

Function

The **neighbor route-refresh** command configures route refreshing for neighbors.
The **no neighbor route-refresh** command cancels the configuration.

Format

- **neighbor** *ipv4-address* **route-refresh**
- **no neighbor** *ipv4-address* **route-refresh**
- **neighbor** *ipv6-address* **route-refresh**
- **no neighbor** *ipv6-address* **route-refresh**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.
ipv6-address	Specifies the IPv6 address of a neighbor.	The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.

Default Value

None

View

BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Configure route refreshing for neighbors.

```
switch(config-bgp)#neighbor 1.1.1.1 route-refresh
switch(config-bgp)#
```

Related Commands

None

4.6.31 neighbor send-community

Function

The **neighbor send-community** command enables sending of the community attribute to a peer.
The **no neighbor send-community** command cancels sending of the attribute.

Format

- **neighbor** *ipv4-address* **send-community**
- **no neighbor** *ipv4-address* **send-community**
- **neighbor** *ipv6-address* **send-community**
- **no neighbor** *ipv6-address* **send-community**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.
ipv6-address	Specifies the IPv6 address of a neighbor.	The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.

Default Value

None

View

BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Enable sending of the community attribute to a peer.

```
switch(config-bgp)#neighbor 1.1.1.1 send-community
switch(config-bgp)#
```

Related Commands

None

4.6.32 neighbor send-label

Function

The **neighbor send-label** command enables label sending for a specific address family.
The **no neighbor send-label** command cancels sending of the attribute.

Format

- **neighbor** *ipv4-address* **send-label**
- **no neighbor** *ipv4-address* **send-label**
- **neighbor** *ipv6-address* **send-label**
- **no neighbor** *ipv6-address* **send-label**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.
ipv6-address	Specifies the IPv6 address of a neighbor.	The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.

Default Value

None

View

BGP configuration view, address family configuration view

Usage Guidelines

None

Note: You need to access the config-bgp-af node of the address family to configure the neighbor send-label command.

Example

Enable label sending for a specific address family.

```
switch(config-bgp-af-ipv4)#neighbor 1.1.1.1 send-label
switch(config-bgp-af-ipv4)#
```

Related Commands

None

4.6.33 neighbor send route-refresh

Function

The **neighbor send route-refresh** command sends route refreshing information.

Format

- **neighbor** *ipv4-address* **send route-refresh** { **ipv4** | **ipv6** } { **unicast** | **multicast** }
- **neighbor** *ipv6-address* **send route-refresh** { **ipv4** | **ipv6** } { **unicast** | **multicast** }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.
ipv6-address	Specifies the IPv6 address of a neighbor.	The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.
unicast	Specifies unicast.	-
multicast	Specifies multicast.	-

Default Value

None

View

BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Send route refreshing information.

```
switch(config-bgp)#neighbor 1.1.1.1 route-refresh
switch(config-bgp)#
```

Related Commands

None

4.6.34 neighbor shutdown

Function

The **neighbor shutdown** command prohibits session establishment with a peer.
The **no neighbor shutdown** command cancels the configuration.

Format

- **neighbor** *ip-address* **shutdown**
- **no neighbor** *ip-address* **shutdown**

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 or IPv6 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255. The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.

Default Value

None

View

BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Prohibit session establishment with a peer.

```
switch(config-bgp)#neighbor 1.1.1.1 shutdown
switch(config-bgp)#
```

Related Commands

None

4.6.35 neighbor update-source

Function

The **neighbor update-source** command specifies the source address used for initiating connection.

The **no neighbor update-source** command deletes a connection address.

Format

- **neighbor** *ip-address1* **update-source** *ip-address2*
- **no neighbor** *ip-address1* **update-source**

Parameters

Parameter	Description	Value
ip-address1	Specifies the IPv4 or IPv6 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255. The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.
ip-address2	Specifies the local IPv4 or IPv6 address of a neighbor, that is, the source address.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255. The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.

Default Value

None

View

BGP configuration view, address family configuration view

Usage Guidelines

You are recommended to use this command when creating multiple peers on two switches through multiple links.

Example

Specify the source address used for initiating connection.

```
switch(config-bgp)#neighbor 1.1.1.1 update-source 2.2.2.2
switch(config-bgp)#
```

Related Commands

None

4.6.36 neighbor valid-ttl-hops

Function

The neighbor valid-ttl-hops command applies the GTSM function to a peer.

Format

- **neighbor** *ipv4-address* **valid-ttl-hops** { *hops-value* | **default** }
- **neighbor** *ipv6-address* **valid-ttl-hops** { *hops-value* | **default** }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 1 to 255.
ipv6-address	Specifies the IPv6 address of a neighbor.	The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.
hops-value	Specifies the TTL hops for detection.	The value is an integer ranging from 1 to 255.
default	Specifies the default value.	255

Default Value

By default, the reauthentication interval is 255.

View

BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Apply the GTSM function to a peer.

```
switch(config-bgp)#neighbor 10.10.12.11 valid-ttl-hops 10
switch(config-bgp)#
```

Related Commands

None

4.6.37 neighbor allow-as-loop

Function

The **neighbor allow-as-loop** command configures the number of repetitions of a local AS number.

Format

- **neighbor** *ipv4-address* **allow-as-loop** { *loop-number* | **default** }
- **neighbor** *ipv6-address* **allow-as-loop** { *loop-number* | **default** }

Parameters

Parameter	Description	Value
ipv4-address	IPv4 address of the neighbor	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.
ipv6-address	Specifies the IPv6 address of a neighbor.	The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.
loop-number	Specifies the number of repetitions of a local AS number.	The value is an integer ranging from 0 to 10.
default	Specifies the default value.	0

Default Value

0

View

BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Configure the number of repetitions of a local AS number.

```
switch(config-bgp)#neighbor 1.1.1.1 allow-as-loop 5
switch(config-bgp)#
```

Related Commands

None

4.6.38 neighbor public-as-only

Function

The **neighbor public-as-only** command configures a BGP update packet to carry only a public AS number, without a private AS number.
The **no neighbor public-as-only** command configures a BGP update packet to carry a private AS number.

Format

- **neighbor** *ipv4-address* **public-as-only**
- **no neighbor** *ipv4-address* **public-as-only**
- **neighbor** *ipv6-address* **public-as-only**
- **no neighbor** *ipv6-address* **public-as-only**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.
ipv6-address	Specifies the IPv6 address of a neighbor.	The IPv6 address contains 128 bits, indicated by 16-bit hexadecimal numbers separated by colons.

Default Value

None

View

BGP configuration view, address family configuration view

Usage Guidelines

Generally, all BGP update packets sent by BGP carry AS numbers (public or private AS numbers).
After this command is configured, if the AS path attribute of BGP routing information contains only private AS numbers, BGP deletes these private AS numbers and then advertises the routing information.

Example

Configure a BGP update packet to carry only a public AS number, without a private AS number.

```
switch(config-bgp)#neighbor 1.1.1.1 public-as-only
switch(config-bgp)#
```

Related Commands

None

4.6.39 preference

Function

The **preference** command sets the protocol priorities of external, internal, and local routes.

Format

- **preference** { *preference1* | **default** } { *preference2* | **default** } { *preference3* | **default** }

Parameters

Parameter	Description	Value
preference1	Specifies the protocol priority of EBGP external routes. External routes are the best routes learned from peers outside the	The value is an integer ranging from 1 to 255. A smaller value indicates a higher priority.

Parameter	Description	Value
	autonomous system.	
Preference2	Specifies the protocol priority of IBGP internal routes. Internal routes are learned from other peers in the autonomous system.	The value is an integer ranging from 1 to 255. A smaller value indicates a higher priority.
Preference3	Specifies the protocol priority of BGP local routes.	The value is an integer ranging from 1 to 255. A smaller value indicates a higher priority.

Default Value

By default, ECMP load balancing is disabled.

View

BGP configuration view, BGP-IPv4 unicast/multicast address family view, BGP-IPv6 unicast address family view, BGP-VPNv4 address family view

Usage Guidelines

You can use this command to configure the BGP protocol priority, to affect the route selection between BGP and other routing protocols.
Routing policies allow you to configure priorities for the routes received from peers that meet the matching conditions. For routes that do not meet the matching conditions, the default priority is used. A smaller priority value indicates a higher priority.

Example

Set the protocol priorities of external, internal, and local routes to 10, 20, and 30 respectively.

```
switch(config-bgp)#preference 10 20 30
switch(config-bgp)#
```

Related Commands

None

4.6.40 router-id

Function

The **router-id** command specifies an ID for the switch.
The **no router-id** command deletes a configured ID.

Format

- **router-id** *router-id*
- **no router-id**

Parameters

Parameter	Description	Value
router-id	Specifies a router ID.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.

Default Value

None

View

BGP configuration view

Usage Guidelines

After BGP is enabled, a route ID is generated. If no route ID is configured, the system automatically uses the maximum loopback address. If no loopback address is available, the maximum IP address of the system is used. Each ID can only identify one switch in the AS.

Example

Specify an ID for the switch.

```
switch(config-bgp)#router-id 10.10.10.10
switch(config-bgp)#
switch(config-bgp)#no router-id
switch(config-bgp)#
```

Related Commands

None

4.6.41 redistribute

Function

The **redistribute** command configures route redistribution.

Format

- **redistribute** { **static** | **connected** | **isis** | **ospf** }
- **redistribute** { **static** | **connected** | **isis** | **ospf** } **med** *med-value*
- **no redistribute** { **static** | **connected** | **isis** | **ospf** }

Parameters

Parameter	Description	Value
med-value	Specifies a MED value.	The value is an integer ranging from 1 to 4294967295.
static | connected | isis |	Specifies the static, direct connect,	-

Parameter	Description	Value
ospf	ISIS, and OSPF routes.	

Default Value

None

View

BGP configuration view, address family configuration view

Usage Guidelines

By default, BGP does not send non-BGP routing information. To enable BGP to send non-BGP routing information, you must configure route redistribution for BGP.
If MED is configured, only the routes with the specified MED value are redistributed when you run this command.

Example

Configure route redistribution.

```
switch(config-bgp)#redistribute isis med 1000
switch(config-bgp)#
```

Related Commands

None

4.6.42 redistribute route-policy

Function

The **redistribute route-policy** command configures route redistribution.

Format

- **redistribute** { **static** | **connected** | **isis** | **ospf** } **route-policy** *route-policy-name*
- **no redistribute** { **static** | **connected** | **isis** | **ospf** } **route-policy** *route-policy-name*

Parameters

Parameter	Description	Value
route-policy-name	Specifies the name of a routing policy.	The value is a string.
static | connected | isis | ospf	Specifies the static, direct connect, ISIS, and OSPF routes.	-

Default Value

None

View

BGP configuration view, address family configuration view

Usage Guidelines

By default, BGP does not send non-BGP routing information. To enable BGP to send non-BGP routing information, you must configure route redistribution for BGP.

Example

Configure route redistribution.

```
switch(config-bgp)#redistribute isis route-policy fs
switch(config-bgp)#
```

Related Commands

None

4.6.43 router bgp

Function

The **router bgp** command enables BGP.
The **no router bgp** command disables BGP.

Format

- **router bgp**
- **router bgp** *as-value*
- **no router bgp**

Parameters

Parameter	Description	Value
as-value	Specifies a local AS number.	The value is an integer ranging from 1 to 65535.

Default Value

None

View

Global configuration view

Usage Guidelines

When the AS number of the router is configured, you can use this command to directly enter the BGP view.

Example

Enable and disable BGP.

```
switch(config)#router bgp 100
switch(config-bgp)#
switch(config)#no router bgp
switch(config)#
```

Related Commands

None

4.6.44 reset bgp

Function

The **reset bgp** command resets all BGP connections.

Format

- **reset bgp**

Parameters

None

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Reset all BGP connections.

```
switch(config)#reset bgp
switch(config)#
```

Related Commands

None

4.6.45 show ip bgp route label

Function

The **show ip bgp route label** command displays BGP route labels.

Format

- **show ip bgp route label**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Display BGP route labels.

```
switch(config)#show ip bgp route label
switch(config)#
```

Related Commands

None

4.6.46 show ip bgp aggregate

Function

The **show ip bgp aggregate** command displays BGP aggregate routes.

Format

show ip bgp aggregate

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Display BGP aggregate routes.

```
switch(config-bgp)#show ip bgp aggregate
  Address                          AddrLen   status   Advertise
  1.2.3.1                          19        up       summaryOnly
switch(config-bgp)#
```

Related Commands

None

4.6.47 show ip bgp config

Function

The **show ip bgp config** command displays BGP configuration information.

Format

show ip bgp config

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Display BGP configuration information.

```
switch(config-bgp)#show ip bgp config
```

```
!
!Bgp Configuration
 router bgp 100
 bgp router-id 192.168.0.1
switch(config-bgp)#
```

Related Commands

None

4.6.48 show ip bgp neighbor

Function

The **show ip bgp neighbor** command displays the status of a specified BGP peer.

Format

- **show ip bgp neighbor**
- **show ip bgp neighbor** *ipv4-address*
- **show ip bgp neighbor** *ipv6-address*
- **show ip bgp neighbor orf state**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.
ipv6-address	Specifies the IPv6 address of a neighbor.	The value is in dotted decimal notation, for example, X: X::X: X.

Default Value

None

View

Common user view, privileged user view, global configuration view, BGP configuration view, address family configuration view

Usage Guidelines

If you use this command without specifying any parameter, all BGP peers are displayed.

Example

Display the status of a specified BGP peer.

```
switch(config-bgp)#show ip bgp neighbor
Address    Rmote-AS     State       StateChange
```

```
1.1.1.1      100          Connect       0
switch(config-bgp)#
switch(config-bgp)#show ip bgp neighbor 1.1.1.1
Neighbor Address: 1.1.1.1
Remote AS Number:100
        Local IP Address Obtain Mode:Automatic
        Multihop EBGP:Disable
        Router Reflector Client:No
        Community Mode:Not Send
        Neighbor State:Connect
        State Change:0
        Hold Time:90 seconds
        Keepalive Interval:30 seconds
        Configured Hold Time:90 seconds
        Configured Keepalive Interval:30 seconds
        Min ASOrigination Interval:15 seconds
        Min Advertisement Interval:30 seconds
        ConnectRetry Timer: 20 seconds
        Total Recieved Message:0
        Total Sent Message:0
        Recieved Update Message:0
        Sent Update Message:0
        MD5 Authentication:Not Support
switch(config-bgp)#
```

Related Commands

None

4.6.49 show ip bgp orf

Function

The **show ip bgp orf** command displays BGP ORF information.

Format

- **show ip bgp orf**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Display BGP ORF information.

```
switch(config-bgp)#show ip bgp orf
switch(config-bgp)#
```

Related Commands

None

4.6.50 show ip bgp resource

Function

The **show ip bgp resource** command displays the BGP resource statistics.

Format

show ip bgp resource

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Display the BGP resource statistics.

```
switch(config-bgp)#show ip bgp resource
Bgp global infor 1124 bytes
```

```
Statistic of BGP Rib to IP forwarding table
 Add Route:0,Add Route Fail:0,Delete Route:0,Delete Route Fail:0

Statistic of BGP Resource Protection

Statistic of BGP Socket Operation
 Operation      Total       Fail
 Open           11          0
 Connect        9           0
 Send           3           0
 Receive        0           0

Dynamic Memory Object Table
Description                size          create      creat-fail      delete      delete-fail
StaticNetwork              36            0           0               0           0
LinkNode                   12            0           0               0           0
TreeNode                   16            0           0               0           0
Peer                       4696          1           0               0           0
RtAttribute                304           0           0               0           0
RouteEntry                 72            0           0               0           0
LinearBuffer               0             0           0               0           0
ASPath                     16            0           0               0           0
switch(config-bgp)#
```

Related Commands

None

4.6.51 show ip bgp route

Function

The **show ip bgp route** command displays the details about a BGP route.

Format

- **show ip bgp route**
- **show ip bgp route** *ipv4-address*
- **show ip bgp route** *ipv6-address*

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a neighbor.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of a neighbor.	The value is in dotted decimal notation, for example, X: X::X: X.

Default Value

By default, the BGP routing table is displayed.

View

Common user view, privileged user view, global configuration view, BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Display BGP route information.

```
switch(config-bgp)#show ip bgp route
DstAddr/Prefixlen   Nexthop   Protocol   Med   LocalPre   AsSquence
8.8.8.3/24          5.3.6.1    bgp        1      2          0x5632
switch(config-bgp)#
```

Related Commands

None

4.6.52 show ip bgp summary

Function

The **show ip bgp summary** command command displays the BGP route statistics.

Format

- **show ip bgp summary**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, BGP configuration view, address family configuration view

Usage Guidelines

None

Example

Display the BGP route statistics.

```
switch(config-bgp)#show ip bgp summary
Protocol          Peer              NumberofRoute
BGP               192.1.1.2         100
switch(config-bgp)#
```

Related Commands

None

4.6.53 tcp {server|client} {enable|disable}

Function

The **tcp {server|client} {enable|disable}** command configures the TCP features of BGP.

Format

- **tcp** { **server** | **client** } { **enable** | **disable** }

Parameters

Parameter	Description	Value
(server|client)	Configures the listening port attribute of TCP. Configures the active connection port attribute of TCP.	-
(enable|disable)	Enables the corresponding port attribute. Disables the corresponding port attribute.	-

Default Value

None

View

BGP configuration view

Usage Guidelines

You can use this command to control local BGP not to accept a remote connection request, or not initiate an active request. This command is basically used only for debugging.

Example

Configure the TCP features of BGP.

```
switch(config-bgp)#tcp server enable
```

```
BGP_SERVER_ENABLE,gBgp4.server_open=1
switch(config-bgp)#
```

Related Commands

None

4.6.54 update-size

Function

The **update-size** command configures the maximum number of bits for a BGP update message.

Format

- **update-size** { *max-bytes* | **default** }

Parameters

Parameter	Description	Value
max-bytes	Specifies the maximum number of bits for an update message.	The value is an integer ranging from 128 to 4096.
default	Specifies the default value.	1460

Default Value

1460

View

BGP configuration view

Usage Guidelines

None

Example

Configure the maximum number of bits for a BGP update message.

```
switch(config-bgp)#update-size 200
switch(config-bgp)#
```

Related Commands

None

4.7 ISIS Configuration Commands

4.7.1 area-authentication-mode

Function

The **area-authentication-mode** command configures a mode for authenticating the received Level-1 routing information packets (LSP and SNP) in an ISIS area based on the preset method and password. It can also be used to add authentication information to the sent Level-1 packets.

Format

- **area-authentication-mode** { **all-send-only** | **default** }
- **area-authentication-mode snp-packet** { **authentication-avoid** | **send-only** }

Parameters

Parameter	Description	Value
all-send-only	Encapsulates authentication information for the generated LSP and SNP packets, without checking the received LSP or SNP packets.	-
authentication-avoid	Does not encapsulate authentication information for the generated SNP packets or check the received SNP packets. Encapsulates authentication information for the generated LSP packets and checks the received LSP packets.	-
send-only	Encapsulates authentication information for the generated LSP and SNP packets, and checks the received LSP packets, without checking the received SNP packets.	-

Default Value

None

View

ISIS configuration view

Usage Guidelines

This command is available only for Level-1 or Level-1-2 routers.

Example

Configure a mode for authenticating the received Level-1 routing information packets in an ISIS area based on the preset method and password.

```
switch(config-bgp)#update-size 200
switch(config-bgp)#
```

Related Commands

None

4.7.2 area-password

Function

The **area-password** command configures a password for an ISIS area.
The **no area-password** command cancels a password.

Format

- **area-password** { **simple** | **md5** } { **cipher** | **plain** } *PASSWORD*
- **area-password** { **simple** | **md5** } *PASSWORD*
- **no area-password**

Parameters

Parameter	Description	Value
PASSWORD	Specifies a password.	The value is a string.
cipher | plain	Displays the password in cipher text or plain text.	-

Default Value

None

View

ISIS configuration view

Usage Guidelines

You can use this command on all routers in an area to prevent unauthenticated routes from carrying intrusive wrong routing information into the link state database. This command is available for Level-1 routers.

Example

Configure a password for an ISIS area.

```
switch(config-bgp)#update-size 200
switch(config-bgp)#
```

Related Commands

None

4.7.3 cost-style

Function

The **cost-style** command configures a cost type.

Format

- **cost-style** { **narrow** | **wide** | **compatible** | **narrow-compatible** | **wide-compatible** | **default** } { **level-1** | **level-2** }

Parameters

Parameter	Description	Value
narrow	Indicates the narrow cost type (TLV = 2/128/130).	-
wide	Indicates the wide cost type (TLV = 22/135).	-
compatible	Indicates that routes with a narrow or wide cost type can be sent and received.	-
narrow-compatible	Indicates that routes with a narrow or wide cost type can be received, but only routes with a narrow cost type can be sent.	-
wide-compatible	Indicates that routes with a narrow or wide cost type can be received, but only routes with a narrow cost type can be sent.	-
default	Specifies the default value.	Indicates that routes with a narrow or wide cost type can be received, but only routes with a narrow cost type can be sent.

Default Value

By default, routes with a narrow or wide cost type can be received, but only routes with a narrow cost type can be sent.

View

ISIS configuration view

Usage Guidelines

None

Example

Configure a cost type.

```
switch(config-isis-1)#cost-style narrow level-1
switch(config-isis-1)#
```

Related Commands

None

4.7.4 debug isis

Function

The **debug isis** command enables ISIS debugging.
The **no debug isis** command disables ISIS debugging.

Format

- **debug isis** { **all** | **hello** | **csnp** | **psnp** | **lsp** | **pdu** | **interface** | **adj** | **route4** | **route6** | **restart** | **sync** | **leak** | **tlv** | **spf** | **memory** | **sysmsg** | **sys** | **bfd** | **te** | **alarm** | **timer** | **redist4** | **redist6** | **snpdetail** | **cmd** | **error** | **update** | **routemsg** }
- **no debug isis** { **all** | **hello** | **csnp** | **psnp** | **lsp** | **pdu** | **interface** | **adj** | **route4** | **route6** | **restart** | **sync** | **leak** | **tlv** | **spf** | **memory** | **sysmsg** | **sys** | **bfd** | **te** | **alarm** | **timer** | **redist4** | **redist6** | **snpdetail** | **cmd** | **error** | **update** | **routemsg** }

Parameters

None

Default Value

By default, ISIS debugging is disabled.

View

Privileged user view

Usage Guidelines

You can use this command to view information about the ISIS process and ISIS packets sent and received. This command is used to maintain and debug the ISIS function of the switch.

Example

Enable all ISIS debugging functions.

```
switch#debug isis all
switch#
```

Related Commands

None

4.7.5 default-route-originate

Function

The **domain-authentication-mode** command enables an ISIS router to generate a default route.

Format

- **default-route-originate** { **none** | **level-1** | **level-2** | **level-1-2** }
- **default-route-originate ipv6** { **none** | **level-1** | **level-2** | **level-1-2** }

Parameters

None

Default Value

None

View

ISIS configuration view

Usage Guidelines

This command is available only for Level-1 or Level-2 routers.

Example

Enable an ISIS router to generate a default route.

```
switch(config-isis-1)#default-route-originate level-1
switch(config-isis-1)#
```

Related Commands

None

4.7.6 domain-authentication-mode

Function

The **domain-authentication-mode** command configures a mode for authenticating the received Level-2 routing information packets (LSP and SNP) in an ISIS routing domain based on the preset method and password.

Format

- **domain-authentication-mode** { **all-send-only** | **default** }
- **domain-authentication-mode snp-packet** { **authentication-avoid** | **send-only** }

Parameters

Parameter	Description	Value
all-send-only	Encapsulates authentication information for the generated LSP and SNP packets, without checking the received LSP or SNP packets.	-
authentication-avoid	Does not encapsulate authentication information for the generated SNP packets or check the received SNP packets. Encapsulates authentication information for the generated LSP packets and checks the received LSP packets.	-
send-only	Encapsulates authentication information for the generated LSP and SNP packets, and checks the received LSP packets, without checking the received SNP packets.	-

Default Value

None

View

ISIS configuration view

Usage Guidelines

This command is available only for Level-2 or Level-1-2 routers.

Example

Configure a mode for authenticating the received Level-2 routing information packets in an ISIS routing domain based on the preset method and password.

```
switch(config-isis-1)#domain-authentication-mode all-send-only
switch(config-isis-1)#
```

Related Commands

None

4.7.7 domain-password

Function

The **domain-password** command configures an authentication password for an ISIS routing domain.
The **no domain-password** command cancels an authentication password for an ISIS routing domain.

Format

- **domain-password** { **simple** | **md5** } *PASSWORD*
- **domain-password** { **simple** | **md5** } { **cipher** | **plain** } *PASSWORD*
- **no domain-password**

Parameters

Parameter	Description	Value
PASSWORD	Specifies a password.	The value is a string.

Default Value

None

View

ISIS configuration view

Usage Guidelines

You can use this command on all routers in an area to prevent unauthenticated routes from carrying intrusive wrong routing information into the link state database. This command is available for Level-2 routers.

Example

#configure an authentication password

```
switch(config-isis-1)#domain-password simple 11
switch(config-isis-1)#
```

Related Commands

None

4.7.8 hostname

Function

The **hostname** command configures an ISIS host name.
The **hostname** command deletes an ISIS host name.

Format

- **hostname** *hostname*
- **no hostname**

Parameters

Parameter	Description	Value
hostname	Specifies an ISIS host name.	The value is a string of 1 to 31 characters.

Default Value

None

View

ISIS configuration view

Usage Guidelines

None

Example

Set the ISIS host name to switchisis.

```
switch(config-isis-1)#hostname switchisis
switch(config-isis-1)#
```

Related Commands

None

4.7.9 ignore-lsp-errors

Function

The **ignore-lsp-errors** command configures whether to ignore ISP packet errors.
The no ignore-lsp-errors command disables this function.

Format

- **ignore-lsp-errors** { **level-1** | **level-2** }
- **no ignore-lsp-errors** { **level-1** | **level-2** }

Parameters

None

Default Value

The function is disabled.

View

ISIS configuration view

Usage Guidelines

You can use this command to enable a router to ignore errors of received ISIS link state packets without error correction.

Example

Configure whether to ignore ISP packet errors.

```
switch(config-isis-1)#ignore-lsp-errors level-1
switch(config-isis-1)#
```

Related Commands

None

4.7.10 ip router isis

Function

The **ip router isis** command enables an ISIS routing process on an interface.
The **no ip router isis** command cancels an ISIS routing process on an interface.

Format

- **ip router isis** [*instance-id*]
- **no ip router isis**

Parameters

Parameter	Description	Value
instance-id	Specifies an ISIS instance ID.	The value is an integer ranging from 1 to 16.

Default Value

None

View

VLANIF configuration view, loopback interface configuration view, interface configuration view

Usage Guidelines

You can use this command to enable an ISIS routing process on an interface. If network connection is available, an IP address must be configured for the interface, and the interface routing process name must be the same as the routing process name. The interface routing process name can be left empty when there is only one process. It must be specified when there are multiple areas.

Example

Enable the ISIS routing process with instance ID 10.

```
switch(config-vlanif-100)#ip router isis 10
switch(config-vlanif-100)#
```

Related Commands

None

4.7.11is-type

Function

The **is-type** command configures the router type level.

Format

- **is-type** { **level-1** | **level-1-2** | **level-2** }

Parameters

None

Default Value

The default value is level-1-2 (site or area router).

View

ISIS configuration view

Usage Guidelines

You can use this command to configure the router type level. It is recommended that you configure the router type. You can use level-1 routers in pure CLNS mode, and use level-2-only routers in pure IP mode.

Example

Set the router type level to level-1.

```
switch(config-isis-1)#is-type level-1
switch(config-isis-1)#
```

Related Commands

None

4.7.12 isis bfd {enable|disable}

Function

The **isis bfd {enable|disable}** command enables or disables BFD on a specified ISIS interface and creates a BFD session with default parameters.

Format

- **isis bfd** { **enable** | **disable** }

Parameters

Parameter	Description	Value
enable	Enables BFD on a specified ISIS interface and establishment of a BFD session with default parameters.	-
disable	Disables BFD on a specified ISIS interface and establishment of a BFD session with default parameters.	-

Default Value

Disable

View

VLANIF configuration view, loopback interface configuration view

Usage Guidelines

If BFD is not enabled globally, the BFD parameters on an interface can be configured, but no BFD session will be established. The BFD priority of interfaces is higher than that of processes. If BFD is enabled on an interface, a BFD session will be established based the BFD parameters on the interface.

Example

Enable the BFD function on interface VLAN 1.

```
switch(config-vlanif-1)#isis bfd enable
switch(config-vlanif-1)#
```

Related Commands

None

4.7.13 isis circuit-ext-domain

Function

The **isis circuit-ext-domain** command suppresses the ISIS PDUs out of an interval transmission domain in a specific connection.
The **no isis circuit-ext-domain** command cancels the suppression.

Format

- **isis circuit-ext-domain**
- **no isis circuit-ext-domain**

Parameters

None

Default Value

By default, suppression is disabled.

View

VLANIF configuration view, loopback interface configuration view

Usage Guidelines

None

Example

Suppress the ISIS PDUs out of an interval transmission domain in a specific connection.

```
switch(config-vlanif-100)#isis circuit-ext-domain
switch(config-vlanif-100)#
```

Related Commands

None

4.7.14 isis circuit-level

Function

The **isis circuit-level** command configures the circuit level. The no isis circuit-level command restores the default state level-1-2.

Format

- **isis circuit-level** { **level-1** | **level-1-2** | **level-2** }
- **no isis circuit-level**

Parameters

None

Default Value

The circuit level is level-1-2.

View

VLANIF configuration view, loopback interface configuration view

Usage Guidelines

You can use this command to configure the circuit level for saving bandwidth. Generally, it does not need to be configured.

Example

Set the circuit level to level-2.

```
switch(config-vlanif-100)#isis circuit-level level-2
switch(config-vlanif-100)#
```

Related Commands

None

4.7.15 isis circuit-type

Function

The **isis circuit-type** command configures the ISIS circuit type.

Format

- **isis circuit-type** { **broadcast** | **ppp** }

Parameters

Parameter	Description	Value
broadcast	Indicates the broadcast type.	-
ppp	Indicates the P2P type.	-

Default Value

broadcast

View

VLANIF configuration view, loopback interface configuration view, interface configuration view

Usage Guidelines

None

Example

Set the ISIS circuit type to ppp.

```
switch(config-vlanif-100)#isis circuit-type ppp
switch(config-vlanif-100)#
```

Related Commands

None

4.7.16 isis csnp-interval

Function

The **isis csnp-interval** command configures the interval for sending CSNP packets at a specified level.
The **no isis csnp-interval** command restores the default value.

Format

- **isis csnp-interval** { **level-1** | **level-2** | **ppp** } *interval-value*
- **no isis csnp-interval** { **level-1** | **level-2** | **ppp** }

Parameters

Parameter	Description	Value
interval-value	Specifies the interval for sending CSNP packets.	The value is an integer ranging from 1 to 600, in seconds.
ppp	Indicates the P2P type.	-

Default Value

10

View

VLANIF configuration view, loopback interface configuration view, interface configuration view

Usage Guidelines

CSNP is short for complete sequence number PDU. CSNP packets are sent through designated routers to maintain synchronization with database. This function is unavailable for serial P2P interfaces. If WAN is regarded as a multi-access grid network, it can be used for WAN connection..

Example

#configure the interval for sending CSNP packets at a specified level.

```
switch(config-vlanif-2)#isis csnp-interval level-1 20
switch(config-vlanif-2)#
```

Related Commands

None

4.7.17 isis default-metric

Function

The **isis default-metric** command configures the metric value of an interface. The no isis default-metric restores the default value.

Format

- **isis default-metric** { **level-1** | **level-2** | **ppp** } *metric-value*
- **no isis default- metric** { **level-1** | **level-2** | **ppp** }

Parameters

Parameter	Description	Value
metric-value	Specifies the metric value of a link interface.	The value is an integer ranging from 0 to 63.
default	Specifies the default metric value of a link interface.	10
ppp	Indicates the P2P type.	-

Default Value

10

View

VLANIF configuration view, interface group configuration view

Usage Guidelines

You can use this command to configure the metric value of an interface on a level-1 or level-2 router.

Example

Set the metric value of an interface to 20.

```
switch(config-vlanif-2)#isis default-metric level-1 20
switch(config-vlanif-2)#
```

Related Commands

None

4.7.18 isis fast-sense neighbor

Function

The **isis fast-sense neighbor** command configures the time for fast sensing a neighbor..
The **no isis fast-sense neighbor** command cancels the configuration.

Format

- **isis fast-sense neighbor** { **level-1** | **level-2** | **ppp** } *value*
- **no isis fast-sense neighbor** { **level-1** | **level-2** | **ppp** }

Parameters

Parameter	Description	Value
value	Specifies an interval for sending Hello packets, in ms.	The value is an integer ranging from 200 to 3000.

Default Value

None

View

if-vlan configuration view, if-fe-route configuration view, if-ge-route configuration view, if-xge-route configuration view, if-trunk-route configuration view, if-loopback configuration view

Usage Guidelines

When ISIS BFD is disabled, you can use this command to speed up neighbor state detection and link state convergence. However, the interval for sending neighbor packets on an interface is also shortened, increasing the device load. Therefore, use this command carefully.

Example

Configure the time for fast sensing a neighbor.

```
switch(config-vlanif-2)#isis fast-sense neighbor level-1 20
switch(config-vlanif-2)#
```

Related Commands

None

4.7.19 isis hello-interval

Function

The **isis hello-interval** command configures the interval for sending ISIS Hello packets.
The **no isis hello-interval** command restores the default value.

Format

- **isis hello-interval** { **level-1** | **level-2** | **ppp** } *interval-value*
- **no isis hello-interval** { **level-1** | **level-2** | **ppp** }

Parameters

Parameter	Description	Value
interval-value	Specifies the ISIS handshake interval.	The value is an integer ranging from 3 to 255, in seconds.
default	Specifies the default interval for sending Hello packets.	The default value is 10s.
ppp	Indicates the P2P type.	-

Default Value

10

View

if-vlan configuration view, if-fe-route configuration view, if-ge-route configuration view, if-xge-route configuration view, if-trunk-route configuration view, if-loopback configuration view

Usage Guidelines

You can use this command to configure the interval for sending Hello packets on a level-1 or level-2 router.

Example

Configure the interval for sending ISIS Hello packets.

```
switch(config-vlanif-2)#isis hello-interval level-1 4
switch(config-vlanif-2)#
```

Related Commands

isis hello-multiplier

4.7.20 isis hello-multiplier

Function

The **isis hello-multiplier** command configures the multiplier of the interval for holding an ISIS Hello packet.
The **no isis hello-multiplier** restores the default value.

Format

- **isis hello-multiplier** { **level-1** | **level-2** | **ppp** } *multiple-value*
- **no isis hello- multiplier** { **level-1** | **level-2** | **ppp** }

Parameters

Parameter	Description	Value
multiple-value	Specifies the multiplier of the interval for holding a Hello packet.	The value is an integer ranging from 2 to 100.
default	Specifies the default multiplier of the interval for holding a Hello packet.	3 times
ppp	Indicates the P2P type.	-

Default Value

3

View

VLANIF configuration view, interface group configuration view

Usage Guidelines

You can use this command to configure the multiplier of the interval for holding a Hello packet, indicating the number of ISIS Hello packets lost by a router before it is determined as unreachable.

Example

Configure the multiplier of the interval for holding an ISIS Hello packet.

```
switch(config-vlanif-2)#isis hello-multiplier level-1 20
switch(config-vlanif-2)#
```

Related Commands

isis hello-interval

4.7.21 isis hello padding

Function

The **isis hello padding** command enables padding of an ISIS Hello packet to the MTU on a specific interface.
The **no isis hello padding** cancels the configuration.

Format

- **isis hello padding**
- **no isis hello padding**

Parameters

None

Default Value

None

View

if-vlan configuration view, if-fe-route configuration view, if-ge-route configuration view, if-xge-route configuration view, if-trunk-route configuration view, if-loopback configuration view

Usage Guidelines

You can use this command to enable padding of an ISIS Hello packet to the MTU on a specific interface over the broadcast network.

Example

Enable padding of an ISIS Hello packet to the MTU.

```
switch(config-vlanif-100)#isis hello padding
switch(config-vlanif-100)#
```

Related Commands

None

4.7.22 isis mesh-group

Function

The **isis mesh-group** commands an ISIS mesh group and specifies a group ID, or configures the mesh group to a blocked state.
The **no isis mesh-group** command cancels the configuration.

Format

- **isis mesh-group** *group-value*
- **isis mesh-group blocked**
- **no isis mesh-group**

Parameters

Parameter	Description	Value
group-value	Specifies the ID of an ISIS mesh group.	The value is an integer ranging from 1 to 65535.

Default Value

By default, mesh group configuration is disabled.

View

if-vlan configuration view, if-fe-route configuration view, if-ge-route configuration view, if-xge-route configuration view, if-trunk-route configuration view, if-loopback configuration view

Usage Guidelines

None

Example

Configure an ISIS mesh group and set the group ID to 100.

```
switch(config-vlanif-100)#isis mesh-group 100
switch(config-vlanif-100)#
```

Related Commands

None

4.7.23 isis password

Function

The **isis password** command configures an authentication password for an interface.
The **no isis password** command cancels a configured password.

Format

- **isis password** { **simple** | **md5** } *PASSWORD* { **level-1** | **level-2** | **ppp** }
- **isis password** { **simple** | **md5** } { **cipher** | **plain** } *PASSWORD* { **level-1** | **level-2** | **ppp** }
- **no isis password** { **level-1** | **level-2** | **ppp** }

Parameters

Parameter	Description	Value
PASSWORD	Specifies a password.	-
ppp	Indicates the P2P type.	-

Default Value

None (When the parameter is specified, the default value is level-1.)

View

VLANIF configuration view, loopback interface configuration view

Usage Guidelines

You can use this command to prevent unauthenticated routers from establishing adjacencies with the router, protecting the network against attacks. A level-1 router acts only as a site router, and a level-2 router acts only as an area router.

Example

Configure an authentication password for an interface.

```
switch(config-vlanif-2)#isis password simple 222 level-1
switch(config-vlanif-2)#
```

Related Commands

None

4.7.24 isis passive-interface

Function

The **isis passive-interface** command configures the passive mode for an interface, to prohibit packet sending.
The **no isis passive-interface** command cancels the passive mode of an interface.

Format

- **isis passive-interface**
- **no isis passive-interface**

Parameters

None

Default Value

None

View

if-vlan configuration view, if-fe-route configuration view, if-ge-route configuration view, if-xge-route configuration view, if-trunk-route configuration view, if-loopback configuration view

Usage Guidelines

None

Example

Configure the passive mode for an interface, to prohibit packet sending.

```
switch(config-vlanif-100)#isis passive-interface
switch(config-vlanif-100)#
```

Related Commands

None

4.7.25 isis priority

Function

The **isis prioirty** command configures the priority of a specified router.
The **no isis prioirty** command restores the default value.

Format

- **isis priority** { **level-1** | **level-2** } *priority-value*
- **no isis priority** { **level-1** | **level-2** }

Parameters

Parameter	Description	Value
priority-value	Specifies the priority of a router.	The value is an integer ranging from 0 to 127.

Default Value

64

View

VLANIF configuration view, loopback interface configuration view

Usage Guidelines

You can use this command to configure the priority of a specified router. The priority determines which router on the LAN becomes a designated router or intermediate system, which is usually a router with a higher priority. A router with a priority of 0 can also act as a designated router or intermediate system. When two routers have the same priority, the one with the larger MAC address (system ID) becomes the designated router or intermediate system.

Example

Configure the priority of a specified router.

```
switch(config-vlanif-100)#isis priority level-1 20
switch(config-vlanif-100)#
```

Related Commands

None

4.7.26 isis psnp-interval

Function

The **isis psnp-interval** command configures the interval for sending PSNP packets at a specified level.
The **no isis psnp-interval** command restores the default value.

Format

- **isis psnp-interval** { **level-1** | **level-2** | **ppp** } *interval-value*
- **no isis psnp-interval** { **level-1** | **level-2** | **ppp** }

Parameters

Parameter	Description	Value
interval-value	Specifies the interval for sending PSNP packets in ISIS.	The value is an integer ranging from 1 to 120, in seconds.
ppp	Indicates the P2P type.	-

Default Value

2

View

if-vlan configuration view, if-fe-route configuration view, if-ge-route configuration view, if-xge-route configuration view, if-trunk-route configuration view, if-loopback configuration view

Usage Guidelines

None

Example

Configure the interval for sending PSNP packets at a specified level.

```
switch(config-vlanif-2)#isis psnp-interval level-1 20
switch(config-vlanif-2)#
```

Related Commands

None

4.7.27 isis three-way-handshake

Function

The **isis three-way-handshake** command configures the ISIS three-way handshake function on a VLAN interface.
The **no isis three-way-handshake** command cancels the configuration.

Format

- **isis three-way-handshake**
- **no isis three-way-handshake**

Parameters

None

Default Value

None

View

if-vlan configuration view, if-fe-route configuration view, if-ge-route configuration view, if-xge-route configuration view, if-trunk-route configuration view, if-loopback configuration view

Usage Guidelines

None

Example

Configure the ISIS three-way handshake function on a VLAN interface.

```
switch(config-vlanif-100)#isis three-way-handshake
switch(config-vlanif-100)#
```

Related Commands

None

4.7.28 isis wide-metric

Function

The **isis wide-metric** command configures the metric type.
The **no isis wide-metric** command cancels the metric type configuration.

Format

- **isis wide-metric** { **level-1** | **level-2** | **ppp** } *metric*
- **no isis wide-metric** { **level-1** | **level-2** | **ppp** }

Parameters

Parameter	Description	Value
metric	Specifies the metric value.	The value is an integer ranging from 0 to 16777215.
ppp	Indicates the P2P type.	-

Default Value

10

View

VLANIF configuration view, loopback interface configuration view

Usage Guidelines

None

Example

Configure the metric type.

```
switch(config-vlanif-1)#isis wide-metric level-1 100
switch(config-vlanif-1)#
```

Related Commands

cost-style

4.7.29 lsp-generation max-interval

Function

The **lsp-generation max-interval** command configures the interval for generating LSP packets in a specified ISIS process.

Format

- **lsp-generation max-interval** { *max-interval* | **default** } **init-interval** { *int-interval* | **default** } **incr-interval** { *incr-interval* | **default** } { **level-1** | **level-2** }

Parameters

Parameter	Description	Value
max-interval	Specifies the maximum interval for generating LSP packets (with the same LSP ID).	The value is an integer ranging from 1 to 120, in seconds. The default value is 2.
int-interval	Specifies the initial interval for generating LSP packets.	The value is an integer ranging from 1 to 60000, in ms. By default, this parameter is not used.
incr-interval	Specifies the incremental interval for generating two LSP packets with the same LSP ID.	The value is an integer ranging from 1 to 60000, in ms. By default, this parameter is not used.
level-1	Specifies the interval for generating Level-1 LSP packets. If the level is not specified, the intervals for generating Level-1 and Level-2 LSP packets are configured.	-
level-2	Specifies the interval for generating Level-2 LSP packets. If the level is not specified, the intervals for generating Level-1 and Level-2 LSP packets are configured.	-

Default Value

The default value of max-interval is 2.

View

ISIS configuration view

Usage Guidelines

If the interval for generating LSP packets is excessively long, the neighbors cannot be notified of the changes in local routing information in time, decreasing the network convergence speed.

Example

Set the maximum interval for generating LSP packets in a specified ISIS process to 80s.

```
switch(config-isis-1)#lsp-generation max-interval max-interval 80 level1
switch(config-isis-1)#
```

Related Commands

None

4.7.30 lsp-refresh-interval

Function

The **lsp-refresh-interval** command configures the interval for refreshing link state packets of a router.
The **no lsp-refresh-interval** command restores the default value.

Format

- **lsp-refresh-interval** *interval-value*
- **no lsp-refresh-interval**

Parameters

Parameter	Description	Value
interval-value	Specifies the interval for refreshing link state packets of a router.	The value is an integer ranging from 1 to 65235, in seconds.

Default Value

900

View

ISIS configuration view

Usage Guidelines

You can use this command to configure the interval for refreshing link state packets of a router. The value must be less than the maximum life time of link state packets.

Example

Set the interval for refreshing link state packets of a router to 1000s.

```
switch(config-isis-1)#lsp-refresh-interval 1000
switch(config-isis-1)#
```

Related Commands

max-lsp-lifetime

4.7.31 max-lsp-lifetime

Function

The **max-lsp-lifetime** command configures the maximum life time of link state packets in the database without refreshing. The **no max-lsp-lifetime** command restores the default value.

Format

- **max-lsp-lifetime** *lifetime*
- **no max-lsp-lifetime**

Parameters

Parameter	Description	Value
lifetime	Specifies the maximum life time of link state packets in the database without refreshing.	The value is an integer ranging from 350 to 65535, in seconds.

Default Value

1200

View

ISIS configuration view

Usage Guidelines

You can use this command to configure the maximum life time of link state packets in the database without refreshing. The value must be greater than the interval for refreshing link state packets.

Example

Set the maximum life time of link state packets in the database without refreshing to 2000s.

```
switch(config-isis-1)#max-lsp-lifetime 2000
switch(config-isis-1)#
```

Related Commands

None

4.7.32 net

Function

The **net** command configures an ISIS network entity title for a routing process.
The **no net** command cancels the configuration.

Format

- **net** *network-entity-title*
- **no net** *network-entity-title*

Parameters

Parameter	Description	Value
network-entity-title	Specifies the name (or address) of a network entity title.	-

Default Value

None

View

ISIS configuration view

Usage Guidelines

You can use this command to configure an ISIS network entity title for a routing process. One to three network entity titles can be configured. The last byte n-selector of the network entity title is 0. The title contains 8 to 20 bytes (including 8 and 20). The 6 bytes before n-selector represent the system ID (with a fixed length). All bytes before the system ID represent the area ID. When multiple network entity titles are configured, the system ID must be the same, and an area has multiple area addresses (for area merging or splitting).

Example

Configure an ISIS network entity for routing.

```
switch(config)#router isis 1
switch(config-isis-1)#net 47.004d.0000.0c11.00
```

Related Commands

None

4.7.33 precedence

Function

The **precedence** command configures the priority of the ISIS protocol.

Format

- **precedence** { *value* | **default** }

Parameters

Parameter	Description	Value
value	Specifies the priority of the ISIS protocol.	The value is an integer ranging from 1 to 255. The smaller the value, the higher the priority.
default	Specifies the default priority of the ISIS protocol.	15

Default Value

15

View

ISIS configuration view

Usage Guidelines

A router may run multiple dynamic routing protocols simultaneously, and routes of multiple protocols may reach the same destination. In this case, the router needs to share routing information among these protocols and select routes of them. To resolve this problem, the system sets a priority for each routing protocol. When different protocols find routes to the same destination, the route of the protocol with the higher priority prevails.

Example

Configure the priority of the ISIS protocol.

```
switch(config-isis-1)#precedence 10
switch(config-isis-1)#
```

Related Commands

None

4.7.34 reset isis

Function

The **reset isis** command resets all ISIS instances or a single ISIS instance.

Format

- **reset isis**
- **reset isis** *isis-instance*

Parameters

Parameter	Description	Value
isis-instance	Specifies an ISIS instance ID.	The value is an integer ranging from 1 to 16.

Default Value

None

View

Perform configuration in the global configuration view before you reset ISIS instances.
Perform configuration in the global configuration view or privileged user view after you reset ISIS instances.

Usage Guidelines

None

Example

Reset all ISIS instances.

```
switch(config)#reset isis
switch(config)#
```

Related Commands

None

4.7.35 redistribute

Function

The **redistribute** command redistributes the routes learned by ISIS from direct-connect port, static routes, or other routing protocols.
The **no redistribute** command cancels route redistribution.

Format

- **redistribute** { **connect** | **static** | **rip** | **bgp** | **ospf** | **isis** }
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **ospf** | **isis** } { **level-1** | **level-2** | **level-1-2** }
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **ospf** | **isis** } { **level-1** | **level-2** | **level-1-2** } **route-policy** *policy-name*
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **ospf** | **isis** } **route-policy** *policy-name*
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **ospf** | **isis** } **cost** { *cost-value* | **default** }
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **ospf** | **isis** } **cost** { *cost-value* | **default** } { **level-1** | **level-2** | **level-1-2** }
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **ospf** | **isis** } **cost** { *cost-value* | **default** } { **level-1** | **level-2** | **level-1-2** } **route-policy** *policy-name*
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **ospf** | **isis** } **cost** { *cost-value* | **default** } **route-policy** *policy-name*
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **ospf** | **isis** } **inherit-cost**
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **ospf** | **isis** } **inherit-cost** { **level-1** | **level-2** | **level-1-2** }
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **ospf** | **isis** } **inherit-cost** { **level-1** | **level-2** | **level-1-2** } **route-policy** *policy-name*
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **ospf** | **isis** } **inherit-cost route-policy** *policy-name*
- **redistribute** { **connect** | **static** | **rip** | **bgp** | **ospf** | **isis** } **route-policy** *policy-name*
- **redistribute** { **rip** | **ospf** | **isis** } *isis-instance-id*
- **redistribute** { **rip** | **ospf** | **isis** } *isis-instance-id* { **level-1** | **level-2** | **level-1-2** }
- **redistribute** { **rip** | **ospf** | **isis** } *isis-instance-id* { **level-1** | **level-2** | **level-1-2** } **route-policy** *policy-name*

- **redistribute** { **rip** | **ospf** | **isis** } *isis-instance-id* **cost** { *cost-value* | **default** }
- **redistribute** { **rip** | **ospf** | **isis** } *isis-instance-id* **cost** { *cost-value* | **default** } { **level-1** | **level-2** | **level-1-2** }
- **redistribute** { **rip** | **ospf** | **isis** } *isis-instance-id* **cost** { *cost-value* | **default** } { **level-1** | **level-2** | **level-1-2** } **route-policy** *policy-name*
- **redistribute** { **rip** | **ospf** | **isis** } *isis-instance-id* **cost** { *cost-value* | **default** } **route-policy** *policy-name*
- **redistribute** { **rip** | **ospf** | **isis** } *isis-instance-id* **inherit-cost**
- **redistribute** { **rip** | **ospf** | **isis** } *isis-instance-id* **inherit-cost** { **level-1** | **level-2** | **level-1-2** }
- **redistribute** { **rip** | **ospf** | **isis** } *isis-instance-id* **inherit-cost** { **level-1** | **level-2** | **level-1-2** } **route-policy** *policy-name*
- **redistribute** { **rip** | **ospf** | **isis** } *isis-instance-id* **inherit-cost route-policy** *policy-name*
- **redistribute** { **rip** | **ospf** | **isis** } *isis-instance-id* **route-policy** *policy-name*
- **no redistribute** { **connect** | **static** | **rip** | **bgp** | **ospf** | **isis** }
- **no redistribute** { **connect** | **static** | **rip** | **bgp** | **ospf** | **isis** } **route-policy** *policy-name*
- **no redistribute** { **rip** | **ospf** | **isis** } *isis-instance-id*
- **no redistribute** { **rip** | **ospf** | **isis** } *isis-instance-id* **route-policy** *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a routing policy.	The value is a string of characters of no more than 32 bytes.
isis-instance-id	Specifies an ISIS instance ID.	The value is an integer ranging from 1 to 16.
cost-value	Specifies the cost.	The value is an integer ranging from 0 to 4261412864.

Default Value

None

View

ISIS route configuration view

Usage Guidelines

Redistribution: By default, ISIS does not send non-ISIS routing information. To enable OSPF to send non-ISIS routing information, you must configure route redistribution for ISIS.
You can use this command to advertise the routes learned by ISIS from direct-connect ports to neighbor routers.

Example

Redistribute the routes learned by ISIS from direct-connect ports

```
switch(config-isis-1)#redistribute connect level-1
switch(config-isis-1)#
```

Related Commands

None

4.7.36 no redistribute route-policy

Function

The **no redistribute** command deletes a route redistribution policy.

Format

- **no redistribute** { **connect** | **static** | **rip** | **bgp** | **ospf** | **isis** } **route-policy**
- **no redistribute** { **rip** | **ospf** | **isis** } *isis-instance-id* **route-policy**

Parameters

Parameter	Description	Value
isis-instance-id	Specifies an ISIS instance ID.	The value is an integer ranging from 1 to 16.

Default Value

None

View

ISIS route configuration view

Usage Guidelines

Redistribution: By default, ISIS does not send non-ISIS routing information. To enable ISIS to send non-ISIS routing information, you must configure route redistribution for ISIS.

Example

Delete a route redistribution policy.

```
switch(config-isis-1)#no redistribute connect route-policy
switch(config-isis-1)#
```

Related Commands

None

4.7.37 redistribute level-2 to level-1

Function

The **redistribute level-2 to level-1** command redistributes level-2 routes to level-1.
The **no redistribute level-2 to level-1** command cancels the redistribution of level-2 routes to level-1.

Format

- **redistribute level-2 to level-1**
- **no redistribute level-2 to level-1**

Parameters

None

Default Value

None

View

ISIS route configuration view

Usage Guidelines

None

Example

Redistribute level-2 routes to level-1.

```
switch(config-isis-1)#redistribute level-2 to level-1
switch(config-isis-1)#
```

Related Commands

None

4.7.38 router isis

Function

The **router isis** command enables the ISIS protocol and specifies an ISIS routing process.
The **no router isis** command disables the ISIS protocol.

Format

- **router isis**
- **router isis** *isis-instance-id*
- **no router isis**
- **no router isis** *isis-instance-id*
- **no router isis all**

Parameters

Parameter	Description	Value
isis-instance-id	Specifies an ISIS instance ID.	The value is an integer ranging from 1 to 16.
name	Specifies a VPN instance name.	The value is a string of up to 30 characters.

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to enable the ISIS protocol and specify an ISIS routing process. Only one ISIS routing process can be enabled in the system. Multiple VPN instances can be configured.

Example

Enter the ISIS view of the router.

```
switch(config)#router isis 10
switch(config-isis-10)#
```

Related Commands

None

4.7.39 router-id

Function

The **router-id** command configures a router ID for ISIS.
The **no router-id** command deletes a router ID for ISIS.

Format

- **router-id** *ipv4-address* { **level-1** | **level-2** }
- **no router-id** { **level-1** | **level-2** }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of the VLANIF interface.	The value is in dotted decimal notation.

Default Value

None

View

ISIS configuration view

Usage Guidelines

None

Example

Configure the priority of IPv6 routes for the ISIS protocol.

```
switch(config-isis-1)#router-id 10.1.1.1 level-1
switch(config-isis-1)#
```

Related Commands

None

4.7.40 set-overload-bit

Function

The **set-overload-bit** command configures a router in SPF calculation so that other routers do not use it as an intermediate hop.
The **set-overload-bit on-startup** command configures the LSP overload bit for a non-pseudo node.
The **no set-overload-bit** command cancels the settings.

Format

- **set-overload-bit**
- **set-overload-bit on-startup** *timeout*
- **no set-overload-bit**

Parameters

Parameter	Description	Value
timeout	Specifies the time for holding the overload bit after the system starts.	The value ranges from 5 to 86400, in seconds.

Default Value

None

View

ISIS configuration view

Usage Guidelines

Generally, the overload bit can be set only upon an error of the router. For example, when the router runs out of memory, the link state database may be incomplete, and therefore the routing table is incomplete or incorrect. The overload bit can be added to its LSP packets to tell other routers to ignore the unreliable router during SPF calculation, until the router recovers. In this case, other routers in the ISIS area may find that there is no path to pass through the router. However, the IP and CLNS prefixes directly connected to the router are still available. You can use this command when you expect to connect a router to the ISIS network without actual traffic passing through it. The following is an example:

- ExampleA test router in the laboratory is connected to a mature network.
- A router is configured as an LSP propagation server (for example, used with the mesh group feature on an NBMA network).
- A router acts just as a collection of virtual circuits used for network management. In this case, the network management workstation must be located on a directly connected to the router with the overload bit setting.

Example

Configure the router to not act as an intermediate hop.

```
switch(config-isis-1)#set-overload-bit
switch(config-isis-1)#
```

Related Commands

None

4.7.41 snmp-trap

Function

The **snmp-trap** command enables or disables the ISIS traps.

Format

- **snmp-trap enable**
- **snmp-trap disable**

Parameters

Parameter	Description	Value
enable	Enables the ISIS traps.	-
disable	Disables the ISIS traps.	-

Default Value

None

View

ISIS configuration view

Usage Guidelines

None

Example

Enable SNMP Trap.

```
switch(config-isis-1)#snmp-trap enable
switch(config-isis-1)#
```

Related Commands

None

4.7.42 show ip isis

Function

The **show ip isis** command displays the information about a single ISIS instance or all ISIS instances.

Format

- **show ip isis**
- **show ip isis** *instance-id*

Parameters

Parameter	Description	Value
instance-id	Specifies an ISIS instance ID.	The value is an integer ranging from 1 to 16.

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, ISIS configuration view

Usage Guidelines

None

Example

Display global ISIS information.

```
switch(config)#show ip isis
Protocol information for IS-IS(1)
Max lsp lifetime         : 1200s
Lsp refresh interval     : 900s
Lsp mtu                  : 1492bytes
Area auth-type           : MD5
Domain auth-type         : MD5
 switch(config)#
```

Related Commands

None

4.7.43 show ip isis bfd session

Function

The **show ip isis bfd session** command displays the information about an ISIS BFD session.

Format

- **show ip isis bfd session**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, ISIS configuration view

Usage Guidelines

The command displays session information only when a BFD session is created successfully.

Example

Display the information about an ISIS BFD session.

```
switch(config)#show ip isis bfd session
switch(config)#
```

Related Commands

None

4.7.44 show ip isis config

Function

The **show ip isis config** command displays the basic ISIS configuration.

Format

show ip isis config

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, ISIS configuration view

Usage Guidelines

You can use this command to display the basic ISIS configuration.

Example

Display the basic ISIS configuration.

```
switch#show ip isis config
Version                         :ISIS_VB3.00.10.00
router isis 1
switch#
```

Related Commands

None

4.7.45 show ip isis database

Function

The **show ip isis database** command displays the link state database.
The **show ip isis database {level-1|level-2}** command displays the information about an ISIS database at a specified level.

Format

- **show ip isis database**
- **show ip isis database** { **level-1** | **level-2** } *instance-id*

Parameters

Parameter	Description	Value
instance-id	Specifies an ISIS instance ID.	The value is an integer ranging from 1 to 16.
string	Specifies a string used for filtering the configuration information to be displayed.	The value is a string.
include	Only displays entries with specified strings.	-
exclude	Only displays entries without specified strings.	-
begin	Only displays entries starting with the specified string.	-

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, ISIS configuration view

Usage Guidelines

You can use this command to display the link state database.
The following table describes the important fields.

Field	Description
LSPID	Specifies a link state PDU identifier. The first 6 bytes represent the system ID of the router sending LSP packets. The next byte represents the pseudo network ID (0: LSP describes system links; non-0: LSP is called non-pseudo network LSP). The last byte represents the number of LSP packets (if the data cannot be filled in a single LSP packet, it will be fragmented, and each fragment contains a different number of LSP packets). The asterisk (*) indicates that the LSP identifier is generated by the system.
LSP SeqNum	Specifies the LSP sequence number.
LSP Checksum	Specifies the checksum of the entire LSP packet.
LSP Holdtime	Specifies the effective time for retaining the LSP packets in the database.
ATT	Indicates the Attach bit. (After this bit is set, the L1-only or L1/L2 routers disconnected from the router finds the nearest L2 router.)
P	Indicates the P bit. (It represents the area partitioning function, and currently cannot be set to 0.)
OL	Indicates the Overload bit. (It indicates the congestion status. When it is set to 1, other routers will not use the system as an intermediate hop. a A data packet is sent to the overload router only when the destination of the data packet is directly linked to the overload router.)
Area Address:	Specifies the reachable area address of the router. (It is manually configured for L1 LSPs, and is obtained from the router for L2 LSPs.)
Metric:	Specifies the metric of the adjacency cost between the source router and the advertising router, or the metric of the acquisition cost between the advertising router and the advertising destination.
Various addresses	"IP" indicates the IP subnet to which the router is performing advertisement. "IP-External" indicates a redistributed route.

Example

Display the link state database.

```
switch#show ip isis database
Database Information for IS-IS(1)
                        Level-1 Link State Database
The total number of ip isis 1 database is: 2
#       ID                  Level   Seq      Checksum  Lifetime  Length  ATT/P/OL
1   0001.0001.0001.00-00    1       1        62661     1195      41      0/0/0
2   0001.0001.0001.00-01    1       1        51524     1195      41      0/0/0
                        Level-2 Link State Database
```

```
The total number of ip isis 1 database is: 2
#       ID                    Level   Seq       Checksum  Lifetime  Length  ATT/P/OL
3   0001.0001.0001.00-00      2       1         62661     1195      41      0/0/0
4   0001.0001.0001.00-01      2       1         51524     1195      41      0/0/0
```

Display the information about an ISIS database at a specified level.

```
switch#show ip isis da level-1 2
Database information for IS-IS(2)
Level-1 Link State Database
#       ID                    Level   Seq       Checksum  Lifetime  Length
1       2222.2222.2222.00-00  1       1         54951     511       38
switch#
```

Related Commands

None

4.7.46 show ip isis database count

Function

The **show ip isis database count** command displays the statistics of an ISIS database.

Format

- **show ip isis database count**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, ISIS configuration view

Usage Guidelines

None

Example

Display the statistics of an ISIS database.

```
switch(config)#show ip isis database count
L1 Database Count :2
L2 Database Count :3
```

```
switch(config)#
```

Related Commands

None

4.7.47 show ip isis database verbose

Function

The **show ip isis database verbose** command displays the details about the link state database.

Format

- **show ip isis database verbose**
- **show ip isis database verbose** *lsp-index*

Parameters

Parameter	Description	Value
lsp-index	Specifies an LSP index.	The value is an integer ranging from 1 to 65535.

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, ISIS configuration view

Usage Guidelines

You can use this command to display the details about the link state database.
The following table describes the important fields.

Field	Description
LSPID	Specifies a link state PDU identifier. The first 6 bytes represent the system ID of the router sending LSP packets. The next byte represents the pseudo network ID (0: LSP describes system links; non-0: LSP is called non-pseudo network LSP). The last byte represents the number of LSP packets (if the data cannot be filled in a single LSP packet, it will be fragmented, and each fragment contains a different number of LSP packets). The asterisk (*) indicates that the LSP identifier is generated by the system.
LSP SeqNum	Specifies the LSP sequence number.
LSP Checksum	Specifies the checksum of the entire LSP packet.
LSP Holdtime	Specifies the effective time for retaining the LSP packets in the database.

Field	Description
ATT	Indicates the Attach bit. (After this bit is set, the L1-only or L1/L2 routers disconnected from the router finds the nearest L2 router.)
P	Indicates the P bit. (It represents the area partitioning function, and currently cannot be set to 0.)
OL	Indicates the Overload bit. (It indicates the congestion status. When it is set to 1, other routers will not use the system as an intermediate hop. a A data packet is sent to the overload router only when the destination of the data packet is directly linked to the overload router.)
Area Address:	Specifies the reachable area address of the router. (It is manually configured for L1 LSPs, and is obtained from the router for L2 LSPs.)
Metric:	Specifies the metric of the adjacency cost between the source router and the advertising router, or the metric of the acquisition cost between the advertising router and the advertising destination.
Various addresses	"IP" indicates the IP subnet to which the router is performing advertisement. "IP-External" indicates a redistributed route.

Example

Display the details about the link state database.

```
switch#show ip isis database verbose

                              Database information for IS-IS(1)

                                    Level-1 Link State Database
LSPID                 LSP-LEVEL   LSPSeqNum       Checksum   LifetimeRemain     Length
0001.0001.0001.00-00      1           2               37490       1187               35
          tlv#1 =(129, 2):
          proto:cc.8e.

          tlv#2 =(1, 2):
          area:1-- 10.

                                    Level-2 Link State Database
LSPID                 LSP-LEVEL   LSPSeqNum       Checksum   LifetimeRemain     Length
0001.0001.0001.00-00      2           2               37490       1187               35
          tlv#1 =(129, 2):
          proto:cc.8e.

          tlv#2 =(1, 2):
          area:1-- 10.

switch#
```

Related Commands

None

4.7.48 show ip isis hostname

Function

The **show ip isis hostname** command displays the dynamic host mapping for ISIS.

Format

- **show ip isis hostname**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, ISIS configuration view

Usage Guidelines

None

Example

Display the dynamic host mapping for ISIS.

```
switch#show ip isis hostname
switch#
```

Related Commands

None

4.7.49 show ip isis interface

Function

The **show ip isis interface** command displays the information (or details) about an interface with ISIS enabled.

Format

- **show ip isis interface**
- **show ip isis interface verbose**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, ISIS configuration view

Usage Guidelines

If the authentication type is nonAuth, no password is displayed in the ISIS interface information.

Example

Display ISIS interface information.

```
switch(config)#show ip isis interface

                        Interface information for IS-IS(1)
The total number of isis(1) interface is:1
Interface                CircID   Adminstate   Type          Level MeshEnable   SmallHello
vlan-11                  1        on           broadcast     L1-2   inactive      false switch(config)#
```

Display details about the ISIS interfaces.

```
switch(config)#show ip isis interface verbose
Interface information for IS-IS(1)
Interface     CircID   Adminstate   Type       Level MeshEnable   SmallHello
vlan-2        1        on           ptToPt     L1-2   Set         False
  Ip isis state                 :enabled
  Ipv6 isis state               :disabled
  Ext-domain                    :enabled
  Passive interface             :yes
  Three-way-handshake           :enabled
  Bfd state                     :enabled
  Mesh group                    :65535
  Level-1 metric                :63
  Level-1 wide metric           :16777215
  Level-1 priority              :127
  Level-1 hello multiplier      :100
  Level-1 hello time            :255s
  Level-1 DIS hello time        :1s
  Level-1 flood interval        :30s
  Level-1 LSP retransmit interval :2s
  Level-1 CSNP interval         :600s
  Level-1 PSNP interval         :120s
  Level-1 adjacency number      :0
```

```
  Level-1 level id              :0001.0002.0003
  Level-1 DIS id                :0000.0000.0000.00
  Level-1 auth type               :md5
  Level-1 auth key              :9df3cc012575c84c
  Level-2 metric                :0
  Level-2 wide metric             :0
  Level-2 priority              :0
  Level-2 hello multiplier        :2
  Level-2 hello time              :3s
  Level-2 DIS hello time          :1s
  Level-2 flood interval          :30s
  Level-2 LSP retransmit interval :2s
  Level-2 CSNP interval           :1s
  Level-2 PSNP interval           :1s
  Level-2 adjacency number        :0
  Level-2 level id              :0001.0002.0003
  Level-2 DIS id                :0000.0000.0000.00
  Level-2 auth type               :simple
  Level-2 auth key              :9df3cc012575c84c
switch(config)#
```

Related Commands

None

4.7.50 show ip isis neighbor

Function

The **show ip isis neighbor** command displays ISIS neighbor information.

Format

- **show ip isis neighbor**
- **show ip isis neighbor verbose**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, ISIS configuration view

Usage Guidelines

None

Example

Display ISIS neighbor information.

```
switch#show ip isis neighbor
                        Neighbor information for IS-IS(1)
The total number of isis(1) neighbor is:2
Interface     Level       ID          MAC        Priority    HoldTime    UpTime            Name
vlan-1111     L1    0020.0200.2002    0005.6890.ffff    64      19       0 days 0:00:20    ---
vlan-1111     L2    0020.0200.2002    0005.6890.ffff    64      29       0 days 12:00:19 AM    ---
switch#
```

Display detailed ISIS neighbor information.

```
switch# show ip isis neighbors verbose
Neighbor information for IS-IS(1)
   Neighbor sequence          : 1
   Interface                  : vlan-20
   Level                      : L2
   System ID                  : 0002.0002.0002
   State                      : up
   Support protocol           : iso,ip
   Area                       : 47
   Ip/Ipv6                    : 192.1.2.100
   System type                : L1L2IntermediateSystem
   3way state                 : up
   Life time                  : 30s
   Life time remain           : 8s
   Extend cid                 : 0

   Neighbor sequence          : 2
   Interface                  : vlan-20
   Level                      : L1
   System ID                  : 0002.0002.0002
   State                      : up
   Support protocol           : iso,ip
   Area                       : 47
   Ip/Ipv6                    : 192.1.2.100
   System type                : L1L2IntermediateSystem
   3way state                 : up
   Life time                  : 30s
   Life time remain           : 8s
   Extend cid                 : 0
```

```
switch#
```

Related Commands

None

4.7.51 show ip isis route

Function

The **show ip isis route** command displays the ISIS routing information.

Format

- **show ip isis route**
- **show ip isis route** *dst-ip-address*
- **show ip isis route** { **level-1** | **level-2** }
- **show ip isis route all**

Parameters

Parameter	Description	Value
level-1	Indicates a level-1 ISIS route.	-
level-2	Indicates a level-2 ISIS route.	-
dst-ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, ISIS configuration view

Usage Guidelines

None

Example

#Displays the ISIS routing information

```
switch#show ip isis route
Total number of IP route is :1
level          dest              nexthop              mac            cost
Level-1   192.1.1.0/24      192.1.1.100        e005:c56e:cdaf     20
switch#show ip isis route all
```

```
Total number of IP route is :9
level      dest              nexthop          mac              cost
Level-1    1.1.1.0/24        1.1.1.2          0000:00b8:0001   10
Level-1    1.1.1.0/24        1.2.2.4          0000:00a0:000a   35
Level-1    1.2.2.0/24        1.2.2.4          0000:00a0:000a   10
Level-1    2.2.2.0/24        1.1.1.2          0000:00b8:0001   10
Level-1    2.2.2.0/24        1.2.2.4          0000:00a0:000a   35
Level-1    2.2.3.0/24        1.1.1.2          0000:00b8:0001   10
Level-1    2.2.3.0/24        1.2.2.4          0000:00a0:000a   35
Level-1    5.5.5.0/24        1.2.2.4          0000:00a0:000a   10
Level-1    5.5.5.0/24        1.2.2.4          0000:00a0:000a   25
switch#
```

Related Commands

None

4.7.52 show ip isis spf-tree

Function

The **show ip isis spf-tree** command displays topology information of the SPF tree.

Format

show ip isis spf-tree

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, ISIS configuration view

Usage Guidelines

When the SPF state is Complete, I-SPF calculation is completed, and the generated SPF tree can be used as a reference for route calculation.

Example

Display topology information of the SPF tree.

```
switch#show ip isis spf-tree
                        SPF-tree information for IS-IS(1)
```

```
  Topo  Level  ID    C-NHop2Dest  C-NHop2Root  C-2MNHop  C-2NHop  Role   Nexthop     CID
  0     1      1357.affd.1111.00-00   N/A        N/A       N/A       0        Main     N/A          N/A
  0     1      1357.affd.1111.01-00   N/A        N/A       N/A       10       Main     0000.0000.0000    1
  0     1      1357.affd.1111.02-00   N/A        N/A       N/A       10       Main     0000.0000.0000    2
  0     1      1357.affd.2222.00-00   N/A        N/A       N/A       10       Main     1357.affd.2222    2
                                                                                1357.affd.2222    1
  0     2      1357.affd.1111.00-00   N/A        N/A       N/A       0        Main     N/A          N/A
  0     2      1357.affd.1111.01-00   N/A        N/A       N/A       10       Main     0000.0000.0000    1
  0     2      1357.affd.1111.02-00   N/A        N/A       N/A       10       Main     0000.0000.0000    2
  0     2      1357.affd.2222.00-00   N/A        N/A       N/A       10       Main     1357.affd.2222    2
  1357.affd.2222    1
switch#
```

Related Commands

None

4.7.53 show ip isis statistic

Function

The **show ip isis statistic** command displays ISIS system and interface statistics.

Format

- **show ip isis statistic**
- **show ip isis statistic interface**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, ISIS configuration view

Usage Guidelines

None

Example

Display ISIS statistics.switch((config-vlanif-1)#show ip isis statistic

```
Statistic information for IS-IS(1)
```

```
Level-1 Statistic
   ID Field Length Mismatches          :0
   Auth Type Fails                     :0
   Auth Fails                          :0
   Corrupt LSPs                        :0
   LSP Errors                          :0
   LSP Database Overloads              :0
   Own LSP Purges                      :0
   SeqNum Skips                        :0
   Attmpt To Exceed Max SeqNums        :0
   Manual Address DropFromAreas        :0
   SPF Runs                            :11

Level-2 Statistic
   ID Field Length Mismatches          :0
   Auth Type Fails                     :0
   Auth Fails                          :0
   Corrupt LSPs                        :0
   LSP Errors                          :0
   LSP Database Overloads              :0
   Own LSP Purges                      :0
   SeqNum Skips                        :0
   Attmpt To Exceed Max SeqNums        :0
   Manual Address DropFromAreas        :0
   SPF Runs                            :3
switch((config-vlanif-1)#
switch#show ip isis statistic interface

Statistic information for IS-IS(1)

Interface vlan 2 Statistic
   Level-1 ID Field Length Mismatches  :0
   Level-1 Auth Type Fails             :0
   Level-1 Auth Fails                  :0
   Level-1 MaxAreaAddr Mismatches      :0
   Level-1 Rejected Adjacencies        :0
   Level-1 Adjacency Changes           :0
   Level-1 Init Fails                  :0
   Level-1 Designated IS Changes       :0
   Level-1 Out Hellos                  :111
   Level-1 Out LSPs                    :0
   Level-1 Out CSNPs                   :0
```

```
  Level-1 Out PSNPs                    :0
  Level-1 Out Unknown Packets          :0
  Level-2 ID Field Length Mismatches   :0
  Level-2 Auth Type Fails              :0
  Level-2 Auth Fails                   :0
  Level-2 MaxAreaAddr Mismatches       :0
  Level-2 Rejected Adjacencies         :0
  Level-2 Adjacency Changes            :0
  Level-2 Init Fails                   :0
  Level-2 Designated IS Changes        :0

Interface vlan 3 Statistic
  Level-1 ID Field Length Mismatches   :0
  Level-1 Auth Type Fails              :0
  Level-1 Auth Fails                   :0
  Level-1 MaxAreaAddr Mismatches       :0
  Level-1 Rejected Adjacencies         :0
  Level-1 Adjacency Changes            :0
  Level-1 Init Fails                   :0
  Level-1 Designated IS Changes        :0
  Level-2 ID Field Length Mismatches   :0
  Level-2 Auth Type Fails              :0
  Level-2 Auth Fails                   :0
  Level-2 MaxAreaAddr Mismatches       :0
  Level-2 Rejected Adjacencies         :0
  Level-2 Adjacency Changes            :0
  Level-2 Init Fails                   :0
  Level-2 Designated IS Changes        :0
switch#
```

Related Commands

None

4.7.54 show ip isis virtual-system

Function

The **show ip isis virtual-system** command displays information about the ISIS virtual system.

Format

- **show ip isis virtual-system**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, ISIS configuration view

Usage Guidelines

None

Example

Display information about the ISIS virtual system.

```
switch#show ip isis virtual-system
  Instance   System ID              Index
  1          1111.1111.1111         1
switch#
```

Related Commands

None

4.7.55 summary-address

Function

The **summary-address** command creates a summary address.
The **no summary-address** command cancels a summary address.

Format

- **summary-address** *(A.B.C.D) (A.B.C.D)* { **level-1** | **level-2** }
- **summary-address** *(A.B.C.D) (A.B.C.D)* **metric** { *metric-value* | **default** } { **level-1** | **level-2** }
- **no summary-address** *(A.B.C.D) (A.B.C.D)* { **level-1** | **level-2** }

Parameters

Parameter	Description	Value
A.B.C.D	Specifies the summary IP address.	The value is in dotted decimal notation, for example, A.B.C.D, in which A to D are decimal numbers ranging from 0 to 255.
metric-value	Specifies the metric value of the summary IP address.	The value is an integer ranging from 0 to 63.
default	Specifies the default metric value of the summary IP address.	0

Default Value

By default, route aggregation is disabled in the system.

View

ISIS configuration view

Usage Guidelines

You can use this command to create a summary address. The summary address can contain multiple addresses at a specified level, and routes obtained from other routing protocols can also be summarized. The metric value used to advertise the summary route is the smallest among all the individual routes.

Example

Create a summary address.

```
switch(config-isis-1)#summary-address 10.2.3.1 255.255.255.0
switch(config-isis-1)#
```

Related Commands

None

4.7.56 summary-prefix

Function

The **summary-prefix** command creates an IPv6 summary route for ISIS.
The **no summary-prefix** cancels the summary.

Format

- **summary-prefix** *(X:X::X:X/M)* { **level-1** | **level-2** }
- **summary-prefix** *(X:X::X:X/M)* **metric** { *metric-value* | **default** } { **level-1** | **level-2** }
- **no summary-address** *(X:X::X:X/M)* { **level-1** | **level-2** }

Parameters

Parameter	Description	Value
X:X::X:X/M	Specifies a summary IPv6 address and its mask.	-
metric-value	Specifies the metric value of the summary IP address.	The value is an integer ranging from 0 to 63.
default	Specifies the default metric value of the summary IP address.	0

Default Value

By default, route aggregation is disabled in the system.

View

ISIS configuration view

Usage Guidelines

You can use this command to create a summary address. The summary address can contain multiple addresses at a specified level, and routes obtained from other routing protocols can also be summarized. The metric value used to advertise the summary route is the smallest among all the individual routes.

Example

Generate an ISIS summary route with address 2000::/32.

```
switch(config-isis-1)#summary-prefix 2000::/32 level-1
switch(config-isis-1)#
```

Related Commands

None

4.7.57 traffic-engineer

Function

The **traffic-engineer** command enables the traffic engineer function for ISIS.

Format

traffic-engineer { **enable** | **disable** } { **level-1** | **level-2** }

Parameters

None

Default Value

None

View

ISIS configuration view

Usage Guidelines

None

Example

Enable the traffic engineer function for ISIS.

```
switch(config-isis-1)#traffic-engineer enable
switch(config-isis-1)#
```

Related Commands

None

4.7.58 timer spf

Function

The **timer spf** command configures the interval for calculating SPF routes.

Format

- **timer spf max-interval** *interval-value*

Parameters

Parameter	Description	Value
interval-value	Specifies the interval for calculating SPF routes.	The value is an integer ranging from 5 to 120.

Default Value

5

View

ISIS configuration view

Usage Guidelines

None

Example

Set the interval for calculating SPF routes to 20.

```
switch(config-isis-1)#timer spf 20
switch(config-isis-1)#
```

Related Commands

None

4.7.59 timer spf max-interval init-interval incr-interval

Function

The **timer spf** command configures the parameters of the smart SPF calculation timer.

Format

- **timer spf max-interval** { *max-interval* | **default** } **init-interval** { *init-interval* | **default** } **incr-interval** { *incr-interval* | **default** }

Parameters

Parameter	Description	Value
max-interval	Specifies the maximum interval of the SPF calculation timer.	The value is an integer ranging from 5 to 120.
init-interval	Specifies the initial interval of the SPF calculation timer.	The value is an integer ranging from 1 to 60000.
incr-interval	Specifies the incremental interval of the SPF calculation timer during re-scheduling.	The value is an integer ranging from 1 to 60000.

Default Value

The default values are 5, 50, and 200 respectively.

View

ISIS configuration view

Usage Guidelines

None

Example

Set the maximum interval of the SPF calculation timer to 20.¥

```
switch(config-isis-1)#timer spf max-interval 20
switch(config-isis-1)#
```

Related Commands

None

4.7.60 virtual-system

Function

The **virtual-system** command configures a virtual system ID for ISIS.
The **no virtual-system** command deletes a virtual system ID for ISIS.

Format

- **virtual-system** *sys-id*
- **no virtual-system** *sys-id*

Parameters

Parameter	Description	Value
sys-id	Specifies the virtual system ID of an ISIS process.	The value contains 6 bytes, in the format of XXXX.XXXX.XXXX.

Default Value

By default, no virtual system ID is configured for an ISIS process.

View

ISIS configuration view

Usage Guidelines

Like a common ID, the virtual system ID must be unique in the routing domain.

Example

Configure a virtual system ID for ISIS.

```
switch(config-isis-1)#virtual-system 1111.1111.1111
switch(config-isis-1)#
```

Related Commands

show ip isis virtual-system

4.8 Routing Policy Configuration Commands

4.8.1 apply cost

Function

The **apply cost** command sets the route cost in the routing information.
The **no apply cost** command restores the route cost to the default value.

Format

- **apply cost** *cost-value*
- **apply cost** { **plus** | **minus** } *cost-value*
- **no apply cost**

Parameters

Parameter	Description	Value
cost-value	Specifies the route cost value.	The value is an integer ranging from 0 to 4294967295.
plus	Specifies the increased cost value.	-
minus	Specifies the decreased cost value.	-

Default Value

By default, no route cost is configured.

View

Route-policy configuration view

Usage Guidelines

None

Example

Set the route cost in the routing information to 200.

```
switch(config)#route-policy fs permit node 12
switch(config-route-policy)#apply cost 200
switch(config-route-policy)#
```

Related Commands

None

4.8.2 apply cost-type

Function

The **apply cost-type** command sets the route cost type in the routing information.
The **no apply cost-type** command cancels the route cost type setting.

Format

- **apply cost-type** { **type-1** | **type-2** }
- **no apply cost-type**

Parameters

Parameter	Description	Value
type-1	Indicates that the route is set to OSPF external Type-1.	-
type-2	Indicates that the route is set to OSPF external Type-2.	-

Default Value

By default, the route cost type is not configured.

View

Route-policy configuration view

Usage Guidelines

None

Example

Set the route cost type to OSPF external Type-1.

```
switch(config)#route-policy fs permit node 12
switch(config-route-policy)#apply cost-type type-1
switch(config-route-policy)#
```

Related Commands

None

4.8.3 apply isis

Function

The **apply isis** command configures the action of modifying the level of a route introduced to ISIS in a routing policy.
The **no apply isis** command restores the default configuration.

Format

- **apply isis** { **level-1** | **level-2** | **level-1-2** }
- **no apply isis**

Parameters

Parameter	Description	Value
level-1	Specifies the ISIS route level to Level-1.	-
level-2	Specifies the ISIS route level to Level-2.	-
level-1-2	Specifies the ISIS route level to Level-1-2.	-

Default Value

By default, the action of modifying the level of a route introduced to ISIS is not configured in a routing policy.

View

Route-policy configuration view

Usage Guidelines

To avoid introducing excessive external routes to ISIS and causing extra burden to the device running ISIS, you can apply a routing policy containing this command when introducing routes to ISIS, to modify the route level.

Example

Configure the level of a route introduced to ISIS.

```
switch(config)#route-policy fs permit node 12
switch(config-route-policy)#apply isis level-1
```

```
switch(config-route-policy)#
```

Related Commands

None

4.8.4 apply local-preference

Function

The **apply local-preference** command configures the local priority of a BGP route.
The **no apply local-preference** command cancels the configuration.

Format

- **apply local-preference** *local-priority*
- **no apply local-preference**

Parameters

Parameter	Description	Value
local-priority	Specifies the local priority of a BGP route.	The value is an integer ranging from 0 to 4294967295.

Default Value

By default, the local priority of a BGP route is not configured.

View

Route-policy configuration view

Usage Guidelines

None

Example

Set the local priority of a BGP route to 150.

```
switch(config)#route-policy fs permit node 12
switch(config-route-policy)#apply local-preference 150
switch(config-route-policy)#
```

Related Commands

None

4.8.5 apply origin

Function

The **apply origin** command configures the route source in the routing information.

The **no apply origin** command cancels the configuration.

Format

- **apply origin** { **igp** | **incomplete** }
- **apply origin egp** *as-number*
- **no apply origin**

Parameters

Parameter	Description	Value
igp	Indicates that the BGP routing information source is an internal route.	-
incomplete	Indicates that the BGP routing information source is unknown.	-
egp	Indicates that the BGP routing information source is an external route.	-
as-number	Specifies the AS number of a BGP external route.	The value is an integer ranging from 1 to 65535.

Default Value

By default, no route source is configured in the routing information.

View

Route-policy configuration view

Usage Guidelines

None

Example

Set the route source in the BGP routing information to incomplete.

```
switch(config)#route-policy fs permit node 12
switch(config-route-policy)#apply origin incomplete
switch(config-route-policy)#
```

Related Commands

None

4.8.6 apply ospf

Function

The **apply ospf** command configures the OSPF translation mode.
The **no apply ospf** command cancels the configuration.

Format

- **apply ospf** { **translate** | **not-translate** }
- **no apply ospf**

Parameters

Parameter	Description	Value
translate	Indicates that OSPF works in translation mode.	-
not-translate	Indicates that OSPF works in non-translation mode.	-

Default Value

By default, the OSPF translation mode is not configured.

View

Route-policy configuration view

Usage Guidelines

None

Example

Configure the OSPF translation mode.

```
switch(config)#route-policy fs permit node 12
switch(config-route-policy)#apply ospf translate
switch(config-route-policy)#
```

Related Commands

None

4.8.7 apply preferred-value

Function

The **apply preferred-value** command configures the preferred value of a BGP route.
The **no apply preferred-value** command cancels the configuration.

Format

- **apply preferred-value** *preferred-value*
- **no apply preferred-value**

Parameters

Parameter	Description	Value
preferred-value	Specifies the preferred value of BGP.	The value is an integer ranging from 0 to 65535.

Default Value

By default, the preferred value of a BGP route is not configured.

View

Route-policy configuration view

Usage Guidelines

None

Example

Set the preferred value of a BGP route to 100.

```
switch(config)#route-policy fs permit node 12
switch(config-route-policy)#apply preferred-value 100
switch(config-route-policy)#
```

Related Commands

None

4.8.8 apply tag

Function

The **apply tag** command sets the tag in the routing information.
The **no apply tag** command cancels the tag in the routing information.

Format

- **apply tag** *tag-value*
- **no apply tag**

Parameters

Parameter	Description	Value
tag-value	Specifies the tag in the routing information.	The value is an integer ranging from 0 to 4294967295.

Default Value

By default, the routing information tag is not configured.

View

Route-policy configuration view

Usage Guidelines

For RIP and RIPNG, the maximum value of the tag field is 65535.

Example

Set the tag in the routing information to 200.

```
switch(config)#route-policy fs permit node 12
switch(config-route-policy)#apply tag 200
switch(config-route-policy)#
```

Related Commands

None

4.8.9 debug route-policy

Function

The **debug route-policy** command enables routing policy debugging.
The **no debug route-policy** command disables routing policy debugging.

Format

- **debug route-policy** { **error** | **map** | **config** | **all** }
- **no debug route-policy** { **error** | **map** | **config** | **all** }

Parameters

Parameter	Description	Value
error	Indicates the error information generated during routing policy configuration.	-
map	Indicates the incorrect mapping entries generated during routing policy configuration.	-
config	Indicates the incorrect configuration generated during routing policy matching.	-
all	Indicates all of the preceding error information.	-

Default Value

By default, routing policy debugging is disabled.

View

Privileged user view

Usage Guidelines

You can use this command to maintain and debug routing policies, and therefore facilitating problem locating.

Example

Enable routing policy debugging and display error information generated for the routing policy.

```
switch#debug route-policy error
switch#
```

Related Commands

None

4.8.10 match aspath

Function

The **match aspath** command configures a match rule based on the AS path filter.
The **no match aspath** command deletes a match rule.

Format

- **match aspath** *name*
- **no match aspath** *name*

Parameters

Parameter	Description	Value
name	Specifies the name of an AS path filter.	The value is a string of 1 to 31 characters. The value does not support spaces and is case-sensitive.

Default Value

By default, the match rule based on the AS path filter is not configured.

View

Route-policy configuration view

Usage Guidelines

This command is available only for BGP. Before using this command, run the ip as-path-filter command to define the AS path filter.

Example

Define a routing policy named test and define a match rule for node 10 in the policy by using AS path filter 2.

```
switch(config)#route-policy test permit node 10
switch(config-route-policy)#match aspath a
```

Related Commands

None

4.8.11match cost

Function

The **match cost** command sets a match rule based on the route cost.
The **no match cost** command cancels a match rule based on the route cost.

Format

- **match cost** *cost-value*
- **no match cost**

Parameters

Parameter	Description	Value
cost-value	Specifies the route cost value.	The value is an integer ranging from 0 to 4294967295.

Default Value

By default, the match rule based on the route cost is not configured.

View

Route-policy configuration view

Usage Guidelines

None

Example

Configure the routing information matching route cost 10.

```
switch(config)#route-policy fs permit node 12
switch(config-route-policy)#match cost 10
switch(config-route-policy)#
```

Related Commands

None

4.8.12 match ip|ipv6 filter-list

Function

The **match ip filter-list** command sets the IPv4-based filter rule for matching the destination network segment.
The **match ipv6 filter-list** command sets the IPv6-based filter rule for matching the destination network segment.
The **no match ip filter-list** command cancels the IPv4-based filter rule for matching the destination network segment.
The **no match ipv6 filter-list** command cancels the IPv6-based filter rule for matching the destination network segment.
The **match ip {next-hop|route-source} filter-list** command sets the IPv4-based filter rule for matching the next hop address or source address advertised by the route.

The **match ipv6 {next-hop|route-source} filter-list** command sets the IPv6-based filter rule for matching the next hop address or source address advertised by the route.
The **no match ip {next-hop|route-source} filter-list** command cancels the IPv4-based filter rule for matching the next hop address or source address advertised by the route.
The **no match ipv6 {next-hop|route-source} filter-list** command cancels the IPv6-based filter rule for matching the next hop address or source address advertised by the route.

Format

- **match ip filter-list** *ipv4-filter-list-number*
- **match ipv6 filter-list** *ipv6-filter-list-number*
- **no match ip filter-list**
- **no match ipv6 filter-list**
- **match ip** { **next-hop** | **route-source** } **filter-list** *ipv4-filter-list-number*
- **match ipv6** { **next-hop** | **route-source** } **filter-list** *ipv6-filter-list-number*
- **no match ip** { **next-hop** | **route-source** } **filter-list**
- **no match ipv6** { **next-hop** | **route-source** } **filter-list**

Parameters

Parameter	Description	Value
ipv4-filter-list-number	Specifies the IPv4-based filter number.	The value is an integer ranging from 1001 to 2000.
ipv6-filter-list-number	Specifies the IPv6-based filter number.	The value is an integer ranging from 3001 to 4000.
next-hop	Indicates the next hop address matching the route.	-
route-source	Indicates the source address matching route advertisement.	-

Default Value

By default, the match rule based on any filter is not configured.

View

Route-policy configuration view

Usage Guidelines

Before using this command, you must run the **filter** *rule-number* **ip** *ipv4-address/M* **any** or **filter** *rule-number* **ip6** *ipv6-address/M* **any** command.
The configuration of *ipv4-address/M* and *ipv6-address/M* varies with different requirements.

Application	Value
Matching the destination network segment	ipv4-address/ipv6-address: specifies the destination network segment. *M*: specifies the mask length.

Application	Value
Matching the next-hop address or source address advertising the route	ipv4-address/ipv6-address: specifies the next-hop IP address or source IP address advertising the route. *M*: 32 (IPv4) or 128 (IPv6)

Example

Configure an IPv4-based filter match rule.

```
switch(config)#route-policy fs permit node 12
switch(config-route-policy)#match ip filter-list 1002
switch(config-route-policy)#
```

Related Commands

None

4.8.13 match ip-prefix

Function

The **match ip-prefix** command sets a match rule based on the IP address prefix list.
The **no match ip-prefix** command cancels a match rule based on the IP address prefix list.

Format

- **match ip-prefix** *prefix-name*
- **no match ip-prefix**

Parameters

Parameter	Description	Value
prefix-name	Specifies the name of an IP address prefix list.	The value is a string.

Default Value

By default, no match rule based on an IPv4 address prefix list is not configured.

View

Route-policy configuration view

Usage Guidelines

Before using this command, you must configure an IP address prefix list.

Example

Configure a match rule based on an IPv4 address prefix list.

```
switch#show ip prefix-list
```

```
ip prefix-list : tes
  index: 11         permit 2.2.0.0/16
switch#configure
   %Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
switch(config)#route-policy fs permit node 12
switch(config-route-policy)#match ip-prefix tes
switch(config-route-policy)#
```

Related Commands

None

4.8.14 match ip {next-hop|route-source} ip-prefix

Function

The **match ip {next-hop|route-source} ip-prefix** command sets a match rule based on IP information.
The **no match ip {next-hop|route-source} ip-prefix** command cancels a match rule based on IP information.

Format

- **match ip** { **next-hop** | **route-source** } **ip-prefix** *prefix-name*
- **no match ip** { **next-hop** | **route-source** } **ip-prefix**

Parameters

Parameter	Description	Value
next-hop	Indicates the next hop address matching the route.	-
route-source	Indicates the source address matching route advertisement.	-
prefix-name	Specifies the name of an IP address prefix list.	The value is a string.

Default Value

By default, no match rule based on an IPv4 address prefix list is not configured.

View

Route-policy configuration view

Usage Guidelines

Before using this command, you must configure an IP address prefix list.

Example

Configure a match rule based on IP information.

```
switch#show ip prefix-list
```

```
ip prefix-list : tes
  index: 11         permit 2.2.0.0/16
switch#configure
   %Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
switch(config)#route-policy fs permit node 12
switch(config-route-policy)#match ip next-hop ip-prefix tes
switch(config-route-policy)#
```

Related Commands

None

4.8.15 match ipv6 {address|next-hop|route-source} prefix-list

Function

The **match ipv6 {address|next-hop|route-source} prefix-list** command sets a match rule based on IPv6 information.
The **no match ipv6 {address|next-hop|route-source} prefix-list** command cancels a match rule based on IPv6 information.

Format

- **match ipv6** { **address** | **next-hop** | **route-source** } **prefix-list** *prefix-name*
- **no match ipv6** { **address** | **next-hop** | **route-source** } **prefix-list**

Parameters

Parameter	Description	Value
address	Specifies the destination address matched with IPv6 routing information.	-
next-hop	Indicates the next hop address matching the route.	-
route-source	Indicates the source address matching route advertisement.	-
prefix-name	Specifies the name of an IP address prefix list.	The value is a string.

Default Value

By default, no match rule based on an IPv4 address prefix list is not configured.

View

Route-policy configuration view

Usage Guidelines

Before using this command, you must configure an IP address prefix list.

Example

Configure a match rule based on IPv6 information.

```
switch(config)#show ipv6 prefix-list
ipv6 prefix-list : test
  index: 10        permit 2000::/64                          ge 120        le 128
switch(config)#route-policy fs permit node 12
switch(config-route-policy)#match ipv6 address prefix-list test
switch(config-route-policy)#
```

Related Commands

None

4.8.16 match ipv6 address prefix-list

Function

The **match ipv6 filter-list** command sets the IPv6-based filter rule for matching the destination network segment.
The **no match ipv6 filter-list** command cancels the IPv6-based filter rule for matching the destination network segment.

Format

- **match ipv6 filter-list** *ipv6-filter-list-number*
- **no match ipv6 filter-list**

Parameters

Parameter	Description	Value
ipv6-filter-list-number	Specifies the IPv6-based filter number.	The value is an integer ranging from 2001 to 4000.

Default Value

By default, the match rule based on any filter is not configured.

View

Route-policy configuration view

Usage Guidelines

Before using this command, you must run the **filter** *rule-number* **ip** *ipv4-address/M* **any** or **filter** *rule-number* **ip6** *ipv6-address/M* **any** command.
The configuration of *ipv6-address/M* varies with application requirements.

Application	Value
Matching the destination network segment	ipv4-address/ipv6-address: specifies the destination network segment. *M*: specifies the mask length.
Matching the next-hop address or source address advertising the route	ipv6-address: Specifies the next-hop IPv6 address or source IPv6 address advertising the route. *M*: 32 (IPv4) or 128 (IPv6)

Example

Configure an IPv6-based filter match rule.

```
switch(config)#route-policy fs permit node 12
switch(config-route-policy)#match ipv6 filter-list 3001
switch(config-route-policy)#
```

Related Commands

None

4.8.17 match process

Function

The **match process** command sets a match rule based on a process number.
The **no match process** command cancels the configuration.

Format

- **match process** *process-number*
- **no match process**

Parameters

Parameter	Description	Value
process-number	Specifies the name of an IP address prefix list.	The value is a string of 0 to 2048 characters. The value does not support spaces and is case-sensitive.

Default Value

By default, no match rule based on a process number is not configured.

View

Route-policy configuration view

Usage Guidelines

This command cooperates with the RIP, OSPF, and BGP re-allocation policy commands. When one protocol has multiple instances, you can configure the filter rule to reserve only one instance in compliance with the rule.

Example

Configure a filter rule based on a process ID.

```
switch(config)#route-policy test permit node 10
switch(config-route-policy)#match process 100
```

Related Commands

None

4.8.18 match route-type

Function

The **match route-type** command sets a match rule based on the route type.
The **no match route-type** command cancels a match rule based on the route type.

Format

- **match route-type** { **internal** | **external-type1** | **external-type2** | **external-type1or2** | **nssa-external-type1** | **nssa-external-type2** | **nssa-external-type1or2** }
- **no match route-type** { **internal** | **external-type1** | **external-type2** | **external-type1or2** | **nssa-external-type1** | **nssa-external-type2** | **nssa-external-type1or2** }

Parameters

Parameter	Description	Value
internal	Indicates internal routes, including inter-area or intra-area OSPF routes.	-
external-type1	Indicates external routes of OSPF Type1.	-
external-type2	Indicates external routes of OSPF Type2.	-
external-type1or2	Indicates external OSPF routes.	-
nssa-external-type1	Indicates external routes of OSPF NSSA Type1.	-
nssa-external-type2	Indicates external routes of OSPF NSSA Type2.	-
nssa-external-type1or2	Indicates external routes of OSPF NSSA.	-

Default Value

By default, the match rule based on the route type is not configured.

View

Route-policy configuration view

Usage Guidelines

For the same routing policy node, if multiple match route-type clauses are configured and the clauses are in an "Or" relation, the apply clause action is implemented when any clause is matched.

Example

Configure a rule for matching external routes of OSPF Type1.

```
switch(config)#route-policy fs permit node 12
switch(config-route-policy)#match route-type external-type1
switch(config-route-policy)#
```

Related Commands

None

4.8.19 match tag

Function

The **match tag** command sets a match rule based on the route tag.
The **no match tag** command cancels a match rule based on the route tag.

Format

- **match tag** *tag-value*
- **no match tag**

Parameters

Parameter	Description	Value
tag-value	Specifies the tag value.	The value is an integer ranging from 0 to 4294967295.

Default Value

By default, the match rule based on the route tag is not configured.

View

Route-policy configuration view

Usage Guidelines

For RIP and RIPNG, the maximum value of the tag field is 65535.

Example

Configure OSPF routing information matching route tag 8.

```
switch(config)#route-policy fs permit node 12
switch(config-route-policy)#match tag 8
switch(config-route-policy)#
```

Related Commands

None

4.8.20 route-policy

Function

The **route-policy** command creates a routing policy and enters the Route-Policy view.
The **no route-policy** command deletes a created routing policy. If node-number is not carried, all routing policy nodes in the routing policy are deleted. If node-number is carried, a specified routing policy node in the routing policy is deleted.

Format

- **route-policy** *policy-name* { **permit** | **deny** } **node** *node-number*
- **no route-policy** *policy-name*
- **no route-policy** *policy-name* **node** *node-number*

Parameters

Parameter	Description	Value
policy-name	Specifies the routing policy name. It uniquely identifies a routing policy.	The value is a string containing 1 to 20 characters.
permit	Sets the routing policy match mode to permit.	-
deny	Sets the routing policy match mode to deny. In this mode, the apply clause is not executed.	-
node-number	Specifies the node number of a routing policy.	The value is an integer ranging from 0 to 65535.

Default Value

By default, no routing policy is created.

View

Global configuration view

Usage Guidelines

One routing policy consists of multiple routing policy nodes (node-number).
Multiple nodes in a routing policy are in an "Or" filter relation. That is, on condition that routing information passes the filter by one node, it can pass all nodes in the routing policy, and match test is not implemented on other routing policy nodes. If routing information does not pass the filter by any node, it cannot pass the routing policy.
If one routing policy defines more than one routing policy node, the smaller the node-number, the higher the priority, and the earlier the match test is performed. Each node should have at least one node in permit match mode.
One node-number can contain multiple match and apply clauses.
The match clause defines the match condition for a routing policy node. The apply clause defines the route behavior for filtering. The match clauses are in an "And" filter relation. That is, a route is considered to pass the filter of a routing policy node unless it matches all match clauses of this routing policy node.
In permit mode, the match mode of a specified node is permit. If a route matches all match clauses of a routing policy node, the route passes the test and is processed with a series of specified actions in the apply clause. Otherwise, the route must attend the test of a next routing policy node.

In deny mode, the match mode of a specified node is deny, and the apply clause is not executed. If a route matches all match clauses of a routing policy node, the route fails the test and cannot attend the test of the next routing policy node. Otherwise, the route continues to be tested by the next node.

Example

Configure policy fs with node-number 12 and match mode permit. Enter the routing policy view.

```
switch(config)#route-policy fs permit node 12
switch(config-route-policy)#
```

Related Commands

None

4.8.21 show route-policy

Function

The **show route-policy** command shows the routing information.

Format

- **show route-policy** *policy-name*
- **show route-policy** *policy-name* **node** *node-number*

Parameters

Parameter	Description	Value
policy-name	Specifies the routing policy name.	The value is a string containing 1 to 20 characters.
node-number	Specifies the node number of a routing policy.	The value is an integer ranging from 0 to 65535.

Default Value

None

View

Privileged user view, global configuration view, route-policy configuration view

Usage Guidelines

None

Example

Display configuration of all routing policy nodes.

```
switch#show route-policy
!routepolicy configuration
```

```
route-policy fs permit node 1
   match ip filter-list 3000
   match route-type external-type1
   match cost 234545
route-policy fs permit node 12

   match ip filter-list 1002
   match ipv6 next-hop filter-list 3000
   match ip route-source filter-list 3000
   match route-type internal
switch#
```

Display configuration of a routing policy named fs.

```
switch#show route-policy fs
policyName:fs
    type:permit     node:1
   match ip filter-list 3000
   match route-type external-type1
   match cost 234545
   type:permit     node:12
   match ip filter-list 1002
   match ip next-hop filter-list 3000
   match ip route-source filter-list 3000
   match route-type internal
   match route-type external-type1or2
switch#
```

Display configuration of a routing policy named fs and node 12 under the policy.

```
switch#show route-policy fs node 12
route-policy fs permit node 12
   match ip filter-list 1002
   match ip next-hop filter-list 3000
   match ip route-source filter-list 3000
   match route-type internal
   match route-type external-type1or2
   match route-type nssa-external-type1or2
   match cost 16777215
   match tag 4294967295
   apply cost 16777215
   apply cost-type type-2
   apply tag 4294967295
```

```
switch#
```

Related Commands

None

4.8.22 show route-policy config

Function

The **show route-policy config** command displays the routing policy configuration.

Format

- **show route-policy config**

Parameters

None

Default Value

None

View

Privileged user view, global configuration view, route-policy configuration view

Usage Guidelines

None

Example

Display the routing policy configuration.

```
switch(config-route-policy)#show route-policy config
route-policy a permit node 10
match ipv6 address prefix-list p1
```

Related Commands

None

4.8.23 show route-policy information

Function

The **show route-policy information** command displays global routing policy information.

Format

- **show route-policy information**

Parameters

None

Default Value

None

View

Privileged user view, global configuration view, route-policy configuration view

Usage Guidelines

None

Example

Display global routing policy information.

```
switch(config-route-policy)#show route-policy information
routePolicyMaxNum                  : 100
 routePolicyCurNum                   : 1
 routePolicyNodeMaxNum            : 100
switch(config-route-policy)#
```

Related Commands

None

5. Multicast Commands

5.1 Overview

This chapter introduces the multicast configuration commands of the N-series switch.

5.2 IGMP Snooping Configuration Commands

5.2.1 igmp-snooping drop

Function

The **igmp-snooping drop** command configures the IGMP snooping query or report mode at an interface.

Format

- **igmp-snooping drop** { **report** | **query** | **both** }
- **no igmp-snooping drop**

Parameters

Parameters	Description	Value
report	Indicates the IGMP snooping report mode.	-
query	Indicates the IGMP snooping query mode.	-

Default Value

None

View

Interface configuration view (Ethernet and trunk) and interface group configuration view

Usage Guidelines

Before using this command, run the igmp-snooping {enable|disable}command to enable the multicast listening of the interface.

Example

Configure the IGMP snooping report mode at an interface.

```
switch(config-100ge1/0/1)#igmp-snooping drop report
switch(config-100ge1/0/1)#
```

5.2.2 igmp-snooping {enable|disable}

Function

The **igmp-snooping {enable|disable}** command enables or disables multicast listening at an interface.

Format

- **igmp-snooping** { **enable** / **disable** }

Parameters

Parameters	Description	Value
enable	Enables multicast listening.	-
disable	Disables multicast listening.	-

Default Value

Disable

View

Interface configuration view (Ethernet and trunk), interface group configuration view

Usage Guidelines

None

Example

Enable IGMP snooping at an interface.

```
switch(config)#interface 100gigaethernet 1/0/1
switch(config-100ge1/0/1)#igmp-snooping enable
switch(config-100ge1/0/1)#
```

5.2.3 igmp-snooping fast-leave

Function

The **igmp-snooping fast-leave** command enables or disables the fast leave function at an interface.

Format

- **igmp-snooping fast-leave** { **enable** / **disable** }

Parameters

Parameters	Description	Value
enable	Enables the fast leave function.	-
disable	Disables the fast leave function.	-

Default Value

None

View

Interface configuration view (Ethernet and trunk), interface group configuration view

Usage Guidelines

After the fast leave function is enabled at an interface, the N-series switch will delete the interface from the forwarding entry of a multicast group immediately after receiving an IGMP Leave packet for this group from a host. When only one user host is connected to the interface, the fast leave mechanism enables the switch to release bandwidth resources in a timely manner.
Before using this command, run the **igmp-snooping start** and **igmp-snooping enable** commands in the global configuration view.

Warning: The fast leave is allowed for each multicast member interface in the current VLAN that is connected to only one receiver host. Otherwise, if an interface is connected to multiple receiver hosts, other receiver hosts fail to receive multicast data.

Example

Enable the fast leave function at an interface.

```
switch(config-100ge1/0/1)#igmp-snooping fast-leave enable
switch(config-100ge1/0/1)#
```

5.2.4 igmp-snooping fast-switch {enable|disable}

Function

The **igmp-snooping fast-switch** command enables or disables the fast switch when the stp ring topology changes.

Format

- **igmp-snooping fast-switch** { **enable** / **disable** }

Parameters

Parameters	Description	Value
enable	Enables the fast switch when stp ring topology changes.	-
disable	Disables the fast switch when stp ring topology changes.	-

Default Value

None

View

MVLAN configuration view

Usage Guidelines

None

Example

Enable the fast switch when stp ring topology changes.

```
switch(config-igmpsnoop-mvlan100)#igmp-snooping fast-switch enable
switch(config-igmpsnoop-mvlan100)#
```

5.2.5 igmp-snooping fast-switch query {enable|disable}

Function

The **igmp-snooping fast-switch query {enable|disable}** command enables or disables the common query sending during the fast switch caused by stp ring topology changes.

Format

- **igmp-snooping fast-switch query** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the common query sending during the fast switch caused by stp ring topology changes.	-
disable	Disables the common query sending during the fast switch caused by stp ring topology changes.	-

Default Value

None

View

Global configuration view, MVLAN configuration view

Usage Guidelines

None

Example

Enable the common query sending during the fast switch caused by stp ring topology changes.

```
switch(config)#igmp-snooping fast-switch query enable
switch(config)#
```

5.2.6 igmp-snooping group-address mvlan

Function

The **igmp-snooping group-address mvlan** command creates a pre-joined group.
The **no igmp-snooping group-address mvlan** command deletes a pre-joined group.

Format

- **igmp-snooping group-address** *group-address* **mvlan** *vlan-id*
- **no igmp-snooping group-address** *group-address* **mvlan** *vlan-id*

Parameters

Parameters	Description	Value
group-address	Specifies the IP address of a multicast group.	The value is in the dotted decimal format, for example, A.B.C.D, where A-D are decimal numbers in the range from 0 to 255.
vlan-id	Specifies a VLAN entry.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Create a pre-joined group.

```
switch(config)#igmp-snooping group-address 1.1.1.1 mvlan 100
switch(config)#
```

5.2.7 igmp-snooping max-response-time

Function

The **igmp-snooping max-response-time** command sets the global maximum response time for multicast listening packets.

Format

- **igmp-snooping max-response-time** { *max-response-time* | **default** }

Parameters

Parameters	Description	Value
max-response-time	Specifies the maximum response time.	The value is an integer ranging from 1 to 25, in seconds.
default	default	10 second

Default Value

10 second

View

MVLAN configuration view

Usage Guidelines

The maximum response time provides the following functions:
It can control the deadline for sending the membership report by the host. It can enable the host to rapidly respond to the query packets and avoid traffic congestion due to a large number of packets sent by the host simultaneously.
It can be used to adjust the aging time of member interfaces. When the N-series switch receives an IGMP Report packet from a host, it sets the aging time of the corresponding group member interface to: IGMP robustness count x General query interval + Maximum response time. This command sets the maximum response time used in the formula. You can configure the IGMP robustness count using the **igmp-snooping robust-count** command. You can query the general query interval using the **igmp-snooping query-interval** command.
Before using this command, run the **igmp-snooping start** and **igmp-snooping enable** commands in the global configuration view.

Warning: The value of **max-response-time** must be smaller than that of **query-interva**l.
The value set by this command in the global configuration view is the initial value provided in the MVLAN creation.
The maximum response time should be modified in the MVLAN configuration view.

Example

Configure the global maximum response time for IGMP snooping General Query packets.

```
switch(config-igmpsnoop-mvlan100)#gmp-snooping max-response-time 10
switch(config-igmpsnoop-mvlan100)#
```

5.2.8 igmp-snooping multicast user-vlan

Function

The **igmp-snooping multicast user-vlan** command specifies user VLANs for multicast replication.
The **no igmp-snooping multicast user-vlan** command deletes user VLANs for multicast replication.

Format

- **igmp-snooping multicast user-vlan** *vlan-list*
- **no igmp-snooping multicast user-vlan** *vlan-list*
- **no igmp-snooping multicast user-vlan all**

Parameters

Parameters	Description	Value
vlan-list	Specifies the VLAN list.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

MVLAN configuration view

Usage Guidelines

Before using this command, run the **igmp-snooping start** and **igmp-snooping enable** commands in the global configuration view.

Example

Configure user VLANs for multicast replication.

```
switch(config-igmpsnoop-mvlan100)#igmp-snooping multicast user-vlan 100
switch(config-igmpsnoop-mvlan100)#
```

5.2.9 igmp-snooping multicast-vlan

Function

The **igmp-snooping multicast-vlan** command enables or disables the multicast replication.

Format

- **igmp-snooping multicast-vlan** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the multicast replication.	-
disable	Disables the multicast replication.	-

Default Value

disable

View

MVLAN configuration view

Usage Guidelines

Before using this command, run the **igmp-snooping start** and **igmp-snooping enable** commands in the global configuration view.

Example

Enable the multicast replication.

```
switch(config-igmpsnoop-mvlan100)#igmp-snooping multicast-vlan enable
switch(config-igmpsnoop-mvlan100)#
```

5.2.10 igmp-snooping mvlan

Function

The **igmp-snooping mvlan** command creates or deletes a multicast VLAN (MVLAN) and displays the MVLAN configuration view.

Format

- **igmp-snooping mvlan** *vlan-id*
- **no igmp-snooping mvlan** *vlan-id*

Parameters

Parameters	Description	Value
vlan-id	Specifies a VLAN entry.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

Global configuration view

Usage Guidelines

Before using this command, run the **igmp-snooping start** and **igmp-snooping enable** commands in the global configuration view.

Example

Create a multicast VLAN and enter the MVLAN configuration view.

```
switch(config)#igmp-snooping mvlan 100
switch(config-igmpsnoop-mvlan100)#
```

5.2.11igmp-snooping forwarding-mode {ip|mac}

Function

The **igmp-snooping forwarding-mode {ip|mac}** command sets the multicast data forwarding mode.

Format

- **igmp-snooping forwarding-mode ip**
- **igmp-snooping forwarding-mode mac**

Parameters

Parameters	Description	Value
ip	Forwards multicast data according to the IP address.	-
mac	Forwards multicast data according to the MAC address.	-

Default Value

None

View

MVLAN configuration view

Usage Guidelines

Before using this command, run the **igmp-snooping start** and **igmp-snooping enable** commands in the global configuration view.

Example

Set the multicast data forwarding mode.

```
switch(config-igmpsnoop-mvlan2)#igmp-snooping forwarding-mode ip
switch(config-igmpsnoop-mvlan2)#
```

5.2.12 igmp-snooping group-limit

Function

The **igmp-snooping group-limit** command configures the maximum number of multicast groups on the interface.
The **igmp-snooping group-limit action** command sets the action when the number of multicast groups at an interface exceeds the limit.

Format

- **igmp-snooping group-limit** *group-limit-value*
- **igmp-snooping group-limit** *group-limit-value* **action** { **delay** | **replace** }
- **no igmp-snooping group-limit**

Parameters

Parameters	Description	Value
group-limit-value	Specifies the maximum number of multicast groups on the interface.	The value is an integer ranging from 1 to 2048.
delay	Drop	-
replace	Replace	-

Default Value

None

View

Interface configuration view (Ethernet and trunk) and interface group configuration view

Usage Guidelines

Before using this command, run the igmp-snooping {enable|disable}command to enable the multicast listening of the interface.

Example

Set the maximum number of multicast groups on the interface to 2.

```
switch(config-100ge1/0/1)#igmp-snooping group-limit 2
switch(config-100ge1/0/1)#
```

5.2.13 igmp-snooping group-policy filter-list

Function

The **igmp-snooping group-policy filter-list** command creates the multicast policy on the current multicast VLAN.
The **igmp-snooping group-policy** command deletes a multicast policy applied to the current multicast VLAN.

Format

- **igmp-snooping group-policy filter-list** *acl-number*
- **igmp-snooping group-policy filter-list** *acl-number* **version** *version-list*
- **no igmp-snooping group-policy**

Parameters

Parameters	Description	Value
acl-number	Specifies the number of the ACL bound with a multicast policy.	The value is an integer in the range from 1001 to 2000.
version-list	Specifies the list of applicable multicast listening protocol versions.	The value is an integer in the range from 1 to 3.

Default Value

None

View

MVLAN configuration view

Usage Guidelines

None

Example

Configure a multicast policy within the multicast VLAN.

```
switch(config-igmpsnoop-mvlan1)#igmp-snooping group-policy filter-list 1001 version 1-3
switch(config-igmpsnoop-mvlan1)#
```

5.2.14 igmp-snooping querier {enable|disable}

Function

The **igmp-snooping querier** command enables or disables the querier function on a VLAN.

Format

- **igmp-snooping querier** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the querier function on a VLAN.	-
disable	Disables the querier function on a VLAN.	-

Default Value

disable

MVLAN configuration view

Usage Guidelines

Before using this command, run the **igmp-snooping start** command in the global configuration view.

Example

Enable the querier function on VLAN 2.

```
switch(config-igmpsnoop-mvlan2)#igmp-snooping querier enable
switch(config-igmpsnoop-mvlan2)#
```

5.2.15 igmp-snooping proxy-ip

Function

The **igmp-snooping proxy ip** command configures a multicast proxy IP address.
The **no igmp-snooping proxy ip** command deletes the configured multicast proxy IP address.

Format

- **igmp-snooping proxy-ip** *ip-address*
- **no igmp-snooping proxy-ip**

Parameters

Parameters	Description	Value
ip-address	Specifies the destination IP address.	The value is in the dotted decimal format, for example, A.B.C.D, where A-D are decimal numbers in the range from 0 to 255.

Default Value

None

View

MVLAN configuration view

Usage Guidelines

Before using this command, run the **igmp-snooping start** and **igmp-snooping enable** commands in the global configuration view.

Example

Configure a multicast proxy IP address.

```
switch(config-igmpsnoop-mvlan100)#igmp-snooping proxy-ip 2.2.2.2
switch(config-igmpsnoop-mvlan100)#
```

5.2.16 igmp-snooping proxy-uplink-port

Function

The **igmp-snooping proxy-uplink-port** command enables or disables the prohibition of sending IGMP query messages to a port.

Format

- **igmp-snooping proxy-uplink-port** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enable the prohibition of sending IGMP query messages to a port.	-
disable	Disable the prohibition of sending IGMP query messages to a port.	-

Default Value

None

View

MVLAN configuration view

Usage Guidelines

None

Example

Enable the prohibition of sending IGMP query messages to a port.

```
switch(config-igmpsnoop-mvlan100)#igmp-snooping proxy-uplink-port enable
switch(config-igmpsnoop-mvlan100)#
```

5.2.17 igmp-snooping query-interval

Function

The **igmp-snooping query-interval** command sets the global general query interval for multicast listening.

Format

- **igmp-snooping query-interval** { *query-interval* | **default** }

Parameters

Parameters	Description	Value
query-interval	Specifies the query interval.	The value is an integer in the range from 10 to 65535.
default	Indicates the default.	60 seconds

Default Value

60 seconds

View

Global configuration view

Usage Guidelines

The query-interval provides the following functions:
It is used to configure the interval for sending IGMP general query messages. If the querier function is enabled in a VLAN, you can use this command to set the general query interval. The N-series switch then periodically sends General Query packets to maintain group memberships on interfaces in the VLAN. The smaller the general query interval, the more sensitive the querier will be, and the more resources will be consumed on the N-series switch.

It can be used to adjust the aging time of member interfaces. When the N-series switch receives an IGMP Report packet from a host, it sets the aging time of the corresponding group member interface to: IGMP robustness count x General query interval + Maximum response time. This command sets the general query interval used in the formula. You can configure the IGMP robustness count using the **igmp-snooping robust-count** command. You can configure the maximum response time using the **igmp-snooping max-response-time** command.
Before using this command, run the **igmp-snooping start** and **igmp-snooping enable** commands in the global configuration view.

Example

Set the global IGMP snooping general query interval to 20 seconds.

```
switch(config)#igmp-snooping query-interval 20
switch(config)#
```

5.2.18 igmp-snooping report-suppress

Function

The **igmp-snooping report-suppress** command enables or disables the multicast notification agency function.

Format

- **igmp-snooping report-suppress** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the multicast notification agency function.	-
disable	Disables the multicast notification agency function.	-

Default Value

Disable

View

MVLAN configuration view

Usage Guidelines

After you configure this command, the switch sends a Report or a Leave packet to the upstream device only when the first member joins the multicast group or the last member leaves the multicast group.
Before using this command, run the **igmp-snooping start** and **igmp-snooping enable** commands in the global configuration view.

Example

Enable the multicast notification agency function.

```
switch(config-igmpsnoop-mvlan100)#igmp-snooping report-suppress enable
```

```
switch(config-igmpsnoop-mvlan100)#
```

5.2.19 igmp-snooping require-router-alert

Function

The **igmp-snooping require-router-alert** command configures the Router-Alert checking function of a multicast VLAN.

Format

- **igmp-snooping require-router-alert** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the Router-Alert checking function for the multicast VLAN.	-
disable	Disables the Router-Alert checking function for the multicast VLAN.	-

Default Value

Disable

View

MVLAN configuration view

Usage Guidelines

None

Example

Enable the Router-Alert checking function for the multicast VLAN.

```
switch(config-igmpsnoop-mvlan1)#igmp-snooping require-router-alert enable
switch(config-igmpsnoop-mvlan1)#
```

5.2.20 igmp-snooping robust-count

Function

The **igmp-snooping robust-count** command sets the robustness count, that is, the number of Group-specific Query packets sent by the querier.

Format

- **igmp-snooping robust-count** { *robust-count* | **default** }

Parameters

Parameters	Description	Value
robust-count	Specifies the IGMP robustness count of the current VLAN.	The value is an integer in the range from 2 to 5.
default	Indicates the default.	2

Default Value

None

View

Global configuration view

Usage Guidelines

The IGMP robustness count has the following functions:
It can be used to configure the number of Group-specific Query packets sent by the querier to avoid packet loss. When the N-series switch switch receives an IGMP Leave packet for a group on a host, it sends a specified number of Group-specific Query packets to check whether this group has other members. The number of Group-specific Query packets is specified by the robustness count. You can query the interval for sending Group-specific Query packets using the **igmp-snooping lastmember-queryinterval** command.
It can be used to adjust the aging time of member interfaces. When the N-series switch receives an IGMP Report packet from a host, it sets the aging time of the corresponding group member interface to: IGMP robustness count x General query interval + Maximum response time. This command sets the robustness count used in the formula. You can query the general query interval using the **igmp-snooping query-interval** command. You can configure the maximum response time using the **igmp-snooping max-response-time** command.
Before using this command, run the **igmp-snooping start** and **igmp-snooping enable** commands in the global configuration view.
If you repeatedly run this command in the same configuration view, the new configuration will overwrite the old configuration.

Example

Set the number of Group-specific Query packets.

```
switch(config)#igmp-snooping robust-count 3
switch(config)#
```

5.2.21 igmp-snooping router-aging-time

Function

The **igmp-snooping router-aging time** command sets the global aging time for router interfaces.

Format

- **igmp-snooping router-aging-time** { *router-aging-time* | **default** }

Parameters

Parameters	Description	Value
router-aging-time	Specifies the aging time of the global router port.	The value is an integer ranging from 1 to 1000, in seconds.
default	Indicates the default.	180 seconds

Default Value

180 seconds

View

Global configuration view

Usage Guidelines

When a dynamic router interface receives an IGMP Query packet or PIM Hello packet, the N-series switch switch resets the aging timer of the router interface.
In default situations:
When a dynamic router interface receives an IGMP Query packet, the N-series switch switch resets the aging timer of the router interface to 400 seconds.
When the interface receives a PIM Hello packet and the Holdtime value carried in the packet is larger than the remaining aging time of the router interface, the N-series switch switch resets the aging timer of the router interface to the Holdtime value. If the Holdtime value is smaller than the remaining aging time, the switch does not reset the aging timer of the router interface.
Before using this command, run the **igmp-snooping start** and **igmp-snooping enable** commands in the global configuration view.

Warning: If you repeatedly run this command in the same configuration view, the new configuration will overwrite the old configuration.

Example

Configure the global aging time of router interfaces.

```
switch(config)#igmp-snooping router-aging-time 2
switch(config)#
```

5.2.22 igmp-snooping lastmember-querynumber

Function

The **igmp-snooping lastmember-querynumber** command sets the number of global group-specific query times.

Format

- **igmp-snooping lastmember-querynumber** { *query-number* | **default** }

Parameters

Parameters	Description	Value
query-number	Specifies the number of global group-specific query times.	The value is an integer in the range from 2 to 5.
default	Indicates the default.	0(apply on global)

Default Value

Default value is 0(apply on global）

View

MVLAN configuration view

Usage Guidelines

Before using this command, run the **igmp-snooping start** and **igmp-snooping enable** commands in the global configuration view.

Example

Set the number of global group-specific query times.

```
switch(config-igmpsnoop-mvlan100)#igmp-snooping lastmember-querynumber 5
switch(config-igmpsnoop-mvlan100)#
```

5.2.23 igmp-snooping lastmember-queryinterval

Function

The **igmp-snooping lastmember-queryinterval** command sets the global group-specific query interval.

Format

- **igmp-snooping lastmember-queryinterval** { *query-interval* | **default** }

Parameters

Parameters	Description	Value
query-interval	Specifies the specific query interval.	The value is an integer in the range from 1 to 5 (unit: s).
default	Indicates the default.	Default value is 0 (apply on global)

Default Value

Default value is 0 (apply on global)

View

MVLAN configuration view

Usage Guidelines

Before using this command, run the **igmp-snooping start** and **igmp-snooping enable** commands in the global configuration view.

Example

Set the global group-specific query interval.

```
switch(config-igmpsnoop-mvlan100)#igmp-snooping lastmember-queryinterval 2
switch(config-igmpsnoop-mvlan100)#
```

5.2.24 igmp-snooping send-query source-address

Function

The **igmp-snooping send-query source-address** command configures the source IP address of the query packet in the snooping mode.

Format

- **igmp-snooping send-query source-address** *src-address*
- **igmp-snooping send-query source-address default**

Parameters

Parameters	Description	Value
src-address	Specifies the source IP address of a query packet.	The value is in dotted decimal notation.
default	Uses the default.	-

Default Value

None

View

MVLAN configuration view

Usage Guidelines

None

Example

Configure the source IP address of the query packet in the snooping mode.

```
switch(config-igmpsnoop-mvlan100)#igmp-snooping send-query source-address 123.11.11.10
switch(config-igmpsnoop-mvlan100)#
```

5.2.25 igmp-snooping {start|stop}

Function

The **igmp-snooping start** command globally enables the multicast listening protocol.
The **igmp-snooping stop** command globally disables the multicast listening protocol.

Format

- **igmp-snooping start**
- **igmp-snooping stop**

Parameters

Parameters	Description	Value
start	Enables IGMP snooping globally.	-
stop	Disables IGMP snooping globally.	-

Default Value

disable

View

Global configuration view

Usage Guidelines

None

Example

Enable IGMP snooping globally.

```
switch(config)#igmp-snooping start
switch(config)#
```

5.2.26 igmp-snooping static-group group-address mvlan

Function

The **igmp-snooping static-group group-address mvlan** command configures or deletes a static multicast group at an interface when no multicast service is running.
The **no igmp-snooping static-group** deletes all the static IGMP groups on the interface.
The **no igmp-snooping static-group mvlan** deletes the specified static IGMP groups of MVLAN on the interface.

Format

- **igmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id*
- **igmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id* **user-vlan** *vlan-id*
- **igmp-snooping static-group group-address** *group-address* **source-address** *source-address* **mvlan** *vlan-id*
- **no igmp-snooping static-group**
- **no igmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id*
- **no igmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id* **user-vlan** *vlan-id*
- **no igmp-snooping static-group group-address** *group-address* **source-address** *source-address* **mvlan** *vlan-id*
- **no igmp-snooping static-group mvlan** *vlan-list*

Parameters

Parameters	Description	Value
group-address	Specifies the IP address of an IGMP group.	The multicast address ranges from 224.0.0.0 to 239.255.255.255.
source-address	Specifies the source IP address.	The value is in dotted decimal notation.
vlan-id	Specifies a VLAN ID.	The value is an integer in the range from 1 to 4094.
vlan-list	Specifies the VLAN sequence number.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

Interface configuration view (Ethernet and trunk), interface group configuration view

Usage Guidelines

None

Example

Configure or delete a static multicast group at an interface when no multicast service is running.

```
switch(config-100ge1/0/1)#igmp-snooping static-group group-address 224.0.0.1 mvlan 100
switch(config-100ge1/0/1)#
```

5.2.27 igmp-snooping static-group group-address mvlan user-vlan

Function

The **igmp-snooping static-group group-address mvlan user-vlan** command configures static user VLANs for multicast replication.
The **no igmp-snooping static-group group-address mvlan user-vlan** command deletes specified or all static user VLANs for multicast replication.

Format

- **igmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id* **user-vlan** *vlan-list*
- **no igmp-snooping static-group**
- **no igmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id* **user-vlan** *vlan-list*
- **no igmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id* **user-vlan all**
- **no igmp-snooping static-group mvlan** *vlan-id*

Parameters

Parameters	Description	Value
group-address	Specifies the IP address of an IGMP group.	The value is in the dotted decimal format, for example, A.B.C.D, where A-D are decimal numbers in the range from 0 to 255.
vlan-id	Specifies the multicast VLAN to which the user will join.	The value is an integer in the range from 1 to 4094.
vlan-list	Specifies the list of static VLANs.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

Interface configuration view (Ethernet and trunk), interface group configuration view

Usage Guidelines

None

Example

Configure a static user VLAN for multicast replication.

```
switch(config-100ge1/0/1)#igmp-snooping static-group group-address 224.1.1.1 mvlan 100 user-vlan 1000
switch(config-100ge1/0/1)#
```

5.2.28 igmp-snooping ssm-mapping {enable|disable}

Function

The **igmp-snooping ssm-mapping {enable|disable}** command enables or disables the SSM-Mapping function of the multicast VLAN.

Format

- **igmp-snooping ssm-mapping** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the SSM-Mapping function of the multicast VLAN.	-
disable	Disables the SSM-Mapping function of the multicast VLAN.	-

Default Value

disable

View

MVLAN configuration view

Usage Guidelines

None

Example

#Enable the SSM mapping function in a multicast VLAN.

```
switch(config-igmpsnoop-mvlan100)#igmp-snooping ssm-mapping enable
switch(config-igmpsnoop-mvlan100)#
```

5.2.29 igmp-snooping ssm-mapping filter-list source-address

Function

The **igmp-snooping ssm-mapping filter-list source-address** command configures the SSM-Mapping table of the multicast VLAN.
The **no igmp-snooping ssm-mapping filter-list source-address** command deletes the SSM-Mapping table of the multicast VLAN.

Format

- **igmp-snooping ssm-mapping filter-list** *acl-number* **source-address** *src-ip-address*
- **no igmp-snooping ssm-mapping filter-list** *acl-number* **source-address** *src-ip-address*

Parameters

Parameters	Description	Value
acl-number	Specifies the ACL number.	The value is an integer in the range from 1001 to 2000.
src-ip-address	Specifies the source IP address to be mapped.	The value is in dotted decimal notation.

Default Value

None

View

MVLAN configuration view

Usage Guidelines

None

Example

Configure an SSM mapping entry in a multicast VLAN.

```
switch(config-igmpsnoop-mvlan1)#igmp-snooping ssm-mapping filter-list 1001 source-address 1.1.1.1
switch(config-igmpsnoop-mvlan1)#
```

5.2.30 igmp-snooping uplink-port

Function

The **igmp-snooping uplink-port** command configures or deletes an uplink interface.

Format

- **igmp-snooping uplink-port** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **igmp-snooping uplink-port eth-trunk** *trunk-number*
- **no igmp-snooping uplink-port** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **no igmp-snooping uplink-port eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer such as <1-1>/<0-2>/<1-52>.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.

Default Value

None

View

MVLAN configuration view

Usage Guidelines

None

Example

Configure an uplink interface.

```
switch(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port 10gigaethernet 1/0/1
switch(config-igmpsnoop-mvlan100)#
```

5.2.31 igmp-snooping uplink-port drop-report

Function

The **igmp-snooping uplink-port drop-report** command enables or disables the prohibition of learning multicast table entries from uplink ports.

Format

- **igmp-snooping uplink-port drop-report** { **enable** | **disable**

Parameters

Parameters	Description	Value
enable	Enables the prohibition of learning multicast table entries from uplink ports.	-
disable	Disables the prohibition of learning multicast table entries from uplink ports.	-

Default Value

None

View

MVLAN configuration view

Usage Guidelines

None

Example

Enable the prohibition of learning multicast table entries from uplink ports.

```
switch(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port drop-report enable
switch(config-igmpsnoop-mvlan100)#
```

5.2.32 igmp-snooping uplink-port-limit

Function

The **igmp-snooping uplink-port-limit** command configures the quantity limit for uplink interfaces.

Format

- **igmp-snooping uplink-port-limit** { *uplink-port-limit* | **default** }

Parameters

Parameters	Description	Value
uplink-port-limit	Specifies the uplink port quantity.	The value is an integer ranging from 1 to 256.
default	Uses the default.	1

Default Value

1

View

MVLAN configuration view

Usage Guidelines

None

Example

Configure the quantity limit for uplink interfaces to 100.

```
switch(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port-limit 100
switch(config-igmpsnoop-mvlan100)#
```

5.2.33 igmp-snooping version

Function

The **igmp-snooping version** command sets the multicast version.

Format

- **igmp-snooping version** { **v1** | **v2** /**v3** }

Parameters

Parameters	Description	Value
v1	Indicates multicast version 1.	-
v2	Indicates multicast version 2.	-
v3	Indicates multicast version 3.	-

Default Value

None

View

MVLAN configuration view

Usage Guidelines

None

Example

Set the IGMP snooping version.

```
switch(config-igmpsnoop-mvlan100)#igmp-snooping version v1
switch(config-igmpsnoop-mvlan100)#
```

5.2.34 igmp-snooping workmode

Function

The **igmp-snooping workmode** command sets the multicast listening mode.

Format

- **igmp-snooping workmode** { **igmp-snooping** | **igmp-proxy** }

Parameters

Parameters	Description	Value
igmp-snooping	Indicates the IGMP-snooping mode.	-
igmp-proxy	Indicates the IGMP-proxy mode.	-

Default Value

None

View

MVLAN configuration view

Usage Guidelines

None

Example

Configure the IGMP snooping working mode.

```
switch(config-igmpsnoop-mvlan100)#igmp-snooping workmode igmp-snooping
switch(config-igmpsnoop-mvlan100)#
```

5.2.35 reset igmp-snooping group

Function

The **reset igmp-snooping group** command resets the configuration of IGMP snooping groups.

Format

- **reset igmp-snooping group**

Parameters

None

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Reset the configuration of IGMP snooping groups.

```
switch(config)#reset igmp-snooping group
switch(config)#
```

5.2.36 show igmp-snooping

Function

The **show igmp-snooping** command displays the global IGMP snooping configuration.

Format

- **show igmp-snooping**

Parameters

None

Default Value

This command displays the following information: IGMP snooping status (enabled or disabled), robustness count, global general query interval, global aging time, and line card synchronization status.

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), MVLAN configuration view, interface group configuration view and batch interface group configuration view

Usage Guidelines

None

Example

Display the global IGMP snooping configuration.

```
switch(config)# show igmp-snooping
  Version                          : IGMPSNOOP_VB3.03.00.00
  Igmp-snooping                    : start
  Robustness                       : 2
  Query Interval                   : 60 seconds
  Max Response Time                : 10 seconds
  Lastmember Query Interval        : 1 second
  V2router Aging Time              : 180 seconds

switch(config)#
```

5.2.37 show igmp-snooping config

Function

The **show igmp-snooping config** command displays the IGMP snooping configuration.

Format

- **show igmp-snooping config**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), MVLAN configuration view, interface group configuration view and batch interface group configuration view

Usage Guidelines

None

Example

View the IGMPSnooping configuration.

```
switch(config)# show igmp-snooping config
 igmp-snooping start
 igmp-snooping mvlan 1

 Interface 10ge-1/0/1
```

```
 igmp-snooping enable
 igmp-snooping mvlan 1 uplink-port
switch(config)#
```

5.2.38 show igmp-snooping egress-port

Function

The **show igmp-snooping egress-port** command displays the configuration of IGMP snooping egress interfaces.

Format

- **show igmp-snooping egress-port**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), MVLAN configuration view, interface group configuration view and batch interface group configuration view

Usage Guidelines

This command displays the following information: group address of the egress interface, multicast VLAN ID, interface type, and port type.

Example

Display the configuration of IGMP snooping outbound interfaces.

```
switch(config)#show igmp-snooping egress-port
 Group Address     MVlan Interface          Type      Expires       OutVlan
 1.1.1.1             100     10ge-1/0/1       static      ---           100
 Total Entry(s) : 1
switch(config)#
```

5.2.39 show igmp-snooping egress-port interface

Function

The **show igmp-snooping egress-port interface** command displays the entry of an interface in a static group.

Format

- **show igmp-snooping egress-port interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **show igmp-snooping egress-port interface eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of 1-1/0-2/1-52.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), MVLAN configuration view, interface group configuration view and batch interface group configuration view

Usage Guidelines

None

Example

Display the forwarding entries on interface 10gigaethernet 1/0/1 in static groups.

```
switch(config)#show igmp-snooping egress-port interface 10gigaethernet 1/01
  Group Address : 225.1.1.1
MVlan: 100
Interface : 10ge-1/01
   Type: static
   Expires : 00:00:00
   OutVlan :    5-10
switch(config)#
```

5.2.40 show igmp-snooping egress-port mvlan

Function

The **show igmp-snooping egress-port mvlan** command displays the entries of a multicast VLAN in static groups.

Format

- **show igmp-snooping egress-port mvlan** *mvlan-id*

Parameters

Parameters	Description	Value
mvlan-id	Specify the multicast VLAN ID.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), MVLAN configuration view, interface group configuration view and batch interface group configuration view

Usage Guidelines

None

Example

Display the forwarding entries of multicast VLAN100 in static groups.

```
switch(config)#show igmp-snooping egress-port mvlan 100
 Group Address : 225.1.1.1
MVlan: 100
Interface : 10ge-1/01
  Type: static
  Expires : 00:00:00
  OutVlan :   5-10
switch(config)#
```

5.2.41 show igmp-snooping group

Function

The **show igmp-snooping group** command displays the configuration of a multicast group in IGMP snooping mode.

Format

- **show igmp-snooping group**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), MVLAN configuration view, interface group configuration view and batch interface group configuration view

Usage Guidelines

This command displays the following information: group address, multicast VLAN ID, and member interfaces added to multicast groups.

Example

Display the configuration of IGMP snooping groups.

```
switch(config)#show igmp-snooping group
 Group Address     MVlan    Pre-join    MemNum
 1.1.1.1              100       disable     1
 Total Entry(s) : 1
switch(config)#
```

5.2.42 show igmp-snooping interface

Function

The **show igmp-snooping interface** command displays the configuration of a multicast interface in IGMP snooping mode.

Format

- **show igmp-snooping interface**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), MVLAN configuration view, interface group configuration view and batch interface group configuration view

Usage Guidelines

This command displays the following information: IGMP snooping interface type, IGMP snooping information, fast leave function status, and controllable multicast information (ctrlmode).

Example

Display the configuration of IGMP snooping interfaces.

```
switch(config)#show igmp-snooping interface
   Interface          Igmp-Snooping    Fastleave
   10ge-1/0/1              enable              disable
switch(config)#
```

5.2.43 show igmp-snooping mvlan

Function

The **show igmp-snooping mvlan** command displays IGMP snooping MVLAN configuration.

Format

- **show igmp-snooping mvlan**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), MVLAN configuration view, interface group configuration view and batch interface group configuration view

Usage Guidelines

This command displays the following information: multicast VLAN working mode, multicast VLAN ID, IGMP snooping version, log proxy function status, and user VLANs.

Example

Display IGMP snooping MVLAN configuration.

```
switch(config)#show igmp-snooping mvlan
MVLAN : 1
  Work Mode : snooping
  Version : v2
  Report Suppress : disable
  Leave Suppress : disable
  Forwarding Mode : ip
  Max Response Time : 10
  Require Router Alert : disable
  Querier : disable
  Proxy Ip : 0.0.0.0
  Multicast Vlan : disable
  SSM Mapping : disable
  Lastmember Query Interval : 1
  Lastmember Query Number : 2

switch(config)#
```

5.2.44 show igmp-snooping source-address

Function

The **show igmp-snooping source-address** command displays the multicast source address configuration in IGMP snooping mode.

Format

- **show igmp-snooping source-address**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), MVLAN configuration view, interface group configuration view and batch interface group configuration view

Usage Guidelines

This command displays the following information: multicast source address, multicast VLAN ID, interface type, and port type.

Example

Display the configuration of IGMP snooping source addresses.

```
switch(config)#show igmp-snooping source-address
 Total Entry(s) : 0
switch(config)#
```

5.2.45 show igmp-snooping ssm-mapping

Function

The **show igmp-snooping ssm-mapping** command shows the multicast SSM-Mapping information.

Format

- **show igmp-snooping ssm-mapping**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), MVLAN configuration view, interface group configuration view and batch interface group configuration view

Usage Guidelines

None

Example

Show the multicast SSM-Mapping information.

```
switch(config)#show igmp-snooping ssm-mapping
MVlan       Filter-list      Source Address
1           1001               10.1.1.1
1           1001               10.1.1.2
1           1002               10.2.1.1
switch(config)#
```

5.2.46 show igmp-snooping uplinkport

Function

The **show igmp-snooping uplinkport** command displays the configuration of IGMP snooping uplink interfaces.

Format

- **show igmp-snooping uplinkport**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), MVLAN configuration view, interface group configuration view and batch interface group configuration view

Usage Guidelines

This command displays the following information: uplink interfaces, multicast VLAN ID, and interface type.

Example

Display the configuration of IGMP snooping uplink interfaces.

```
switch(config)# show igmp-snooping uplinkport
  Mvlan    UplinkPort       Expires          Type
```

```
  1            10ge-1/0/1          ---                 static
switch(config)#
```

5.3 IGMP Configuration Command

5.3.1 igmp

Function

igmp command is used to create IGMP public network instance.
no igmp command is used to delete IGMP public network instance.

Format

- **igmp**
- **no igmp**

Parameters

None

Default Value

None

View

Global Configuration View

Usage Guidelines

None

Example

Create IGMP public network instance.

```
switch(config)#igmp
switch(config-igmp)#
```

5.3.2 igmp {enable|disable}

Function

igmp enable command is used to enable IGMP function of interface.
igmp disable command is used to disable IGMP function of interface.

Format

- **igmp** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	make effective	-
disable	make ineffective	-

Default Value

Disabled

View

VLANIF Configuration View

Usage Guidelines

None

Warning: Before configuring IGMP, please first configure the IP address of VLAN interface, or the IGMP function cannot be configured successfully.
Before enabling IGMP of some interface, please first enable the IGMP function of instance for interface, or it will fail.

Example

#Enable IGMP function of interface.

```
switch(config)#interface vlan 100
switch(config-vlanif-100)#igmp enable
switch(config-vlanif-100)#
```

5.3.3 igmp fast-leave

Function

igmp fast-leave enable command is used to enable IGMP fast leaving function of interface.
igmp fast-leave disable command is used to disable IGMP fast leaving function of interface.

Format

- **igmp fast-leave** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	make effective	-
disable	make ineffective	-

Default Value

Disabled

View

VLANIF Configuration View

Usage Guidelines

After enabling IGMP fast leaving function, it will trigger the host to send IGMP leaving message when the multicast member is leaving. When Switch receives the IGMP leaving message, it will delete the multicast forwarding table of interface immediately so as to save the bandwidth and resource and at the same it will realize the service fast switch.
After disabling IGMP fast leaving function, the IGMP querier will send the IGMP specific group query message or IGMP specific source query message when it receives the IGMP leaving message sent by host but will not send the leaving announcement to the upstream directly.

Example

Enable IGMP fast leaving function of interface.

```
switch(config-vlanif-100)#igmp fast-leave enable
switch(config-vlanif-100)#
```

5.3.4 igmp lastmember-queryinterval

Function

The **igmp lastmember-queryinterval** command is used to configure the interval of the IGMP last group member query message sent out on interface when the IGMP querier receives the IGMP leaving message sent by the host.

Format

- **igmp lastmember-queryinterval** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	the interval of the IGMP last group member query message	integer, 1~5, unit: second
default	Default value	The default value is the global dynamic value.

Default Value

The default time interval of sending the last member query packet is the global dynamic value.

View

VLANIF Configuration View

Usage Guidelines

This command is applied to the IGMP querier running IGMPv2 or IGMPv3. This Function (only effective for current interface) is similar to the command of lastmember-queryinterval (globally effective) and only the configuration view is different. System first uses the interface configuration and then uses the configuration in IGMP Configuration View.

In the sharing network of hosts, there may be multiple Switches connected. These multicast Switches spontaneously elect and the winner is called querier to maintain the IGMP group member relationship of interface. When the querier receives the leaving message for some specific multicast group, it will continuously send the specific group query message to query whether there is member in this multicast group. If there are group member in the network, then it must send the Report message in the maximum response time. If during the maximum response time, the querier receives the Report message sent from the host, it will continuously maintain the group member relationship of this group. Or it will think that the last member in the network has been left and not maintain the group member relationship.

Example

#Configure the interval of the IGMP last group member query message sent out on interface when the IGMP querier receives the IGMP leaving message sent by the host.

```
switch(config-vlanif-100)#igmp lastmember-queryinterval 2
switch(config-vlanif-100)#
```

5.3.5 igmp limit

Function

igmp limit command is used to configure the maximum number of IGMP member of interface.

Format

- **igmp limit** { *number* | **default** }

Parameters

Parameters	Description	Value
number	the maximum number of IGMP member of interface	integer, 1-2048
default	Default value	The default value is the global dynamic value.

Default Value

The default value is the global dynamic value.

View

VLANIF Configuration View

Usage Guidelines

When the IGMP table item number reach the limit number, it will not create new IGMP table item. If it needs to add new multicast group, it is recommended to delete some useless item or modify the limit number or join in static multicast group.

Example

#Configure the maximum number of IGMP member of interface.

```
switch(config-vlanif-100)#igmp limit 1000
```

```
switch(config-vlanif-100)#
```

5.3.6 igmp max-response-time

Function

igmp max-response-time command is used to configure the maximum response interval of IGMP query message on interface.

Format

- **igmp max-response-time** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	the maximum response interval of IGMP query message	integer, 1~25, unit: second
default	Default Value	The default value is the global dynamic value.

Default Value

The global dynamic value is inherited for the maximum response time of packet query via IGMP.

View

VLANIF Configuration View

Usage Guidelines

This command is applied to the IGMP querier running IGMPv2 or IGMPv3. This Function (only effective for current interface) is similar to the command of max-response-time (globally effective) and only the configuration view is different. System first uses the interface configuration and then uses the configuration in IGMP Configuration View.

Example

Configure the maximum response interval of IGMP query message on interface.

```
switch(config-vlanif-100)#igmp max-response-time 6
switch(config-vlanif-100)#
```

5.3.7 igmp timer other-querier-present

Function

igmp timer other-querier-present command is used to configure the timeout interval of other IGMP queriers on interface.

Format

- **igmp timer other-querier-present** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	the timeout interval of other IGMP queriers	integer, 1~65535, unit: second
default	Default value	The default value is the global dynamic value.

Default Value

None

View

VLANIF Configuration View

Usage Guidelines

The timeout interval calculation formula of other IGMP querier:
the timeout interval of other IGMP querier = robust × IGMP general group query message sending interval +（1/2）× the maximum response interval of query message
This command is applied to IGMPv2 and IGMPv3. This Function (only effective for current interface) is similar to the command of timer other-querier-present (globally effective) and only the configuration view is different. System first uses the interface configuration and then uses the configuration in IGMP Configuration View.

Warning: If the timeout interval of other IGMP querier is less than the IGMP general group query message sending interval, it will result in repeated change of querier in network. User shold be careful to configure.

Example

Configure the timeout interval of other IGMP queriers on interface.

```
switch(config-vlanif-100)#igmp timer other-querier-present 100
switch(config-vlanif-100)#
```

5.3.8 igmp general-query

Function

igmp general-query command is used to configure the interface to send general query message.

Format

- **igmp general-query**

Parameters

None

Default Value

Not send general query message

View

VLANIF Configuration View

Usage Guidelines

This Function is similar to the command of general-query vlan.
The IGMP querier uses the General Query message to check all connected sub-network periodically so as to determine whether there is group member and to detect when there will be no any group member.

Example

Configure the interface to send general query message.

```
switch(config-vlanif-100)#igmp general-query
switch(config-vlanif-100)#
```

5.3.9 general-query vlan

Function

general-query vlan command is used to globally configure the specific VLAN interface to send general query message.

Format

- **general-query vlan** *vlan-id*

Parameters

Parameters	Description	Value
vlan-id	Specifies the VLAN in which General Query messages are sent.	It is an integer ranging from 1 to 4094.

Default Value

Do not send general query message.

View

IGMP Configuration View

Usage Guidelines

This function is similar to the command of igmp general-query and their difference is the configuration view.
This command only is effective in the instance. The interface belonging to the instane will inherit all configuration of the instance when it is created.

Example

#Configure the specific VLAN interface to send general query message.

```
switch(config-igmp)#general-query vlan 100
switch(config-igmp)#
```

5.3.10 igmp group-policy filter-list

Function

igmp group-policy filter-list command is used to the IGMP group filter of interface to limit host to join the multicast group. **no igmp group-policy** command is used to cancel the IGMP group filter of interface.

Format

- **igmp group-policy filter-list** *acl-number*
- **igmp group-policy filter-list** *acl-number* **version** *version-list*
- **no igmp group-policy**

Parameters

Parameters	Description	Value
acl-number	ACL number	integer, 1001~2000, IPv4ACL
version-list	1: only host of IGMPv1 joins in the multicast group 2: only host of IGMPv2 joins in the multicast group 3: only host of IGMPv3 joins in the multicast group	integer including 1, 2, 3, form as1-3

Default Value

No filter, host can join in any multicast group.

View

VLANIF Configuration View

Usage Guidelines

Before using this command, please first configure ACL to limit the multicast group range which host can join in. When using this command, if not designate IGMP verstion, then the ACL is applied to IGMPv1, v2 and v3 host.

Example

#Configure igmp group-policy filter-list

```
switch(config)#filter-list 1001
switch(configure-filter-ipv4-1001)#filter 1 ip 225.1.1.1/32 any
switch(configure-filter-ipv4-1001)#filter 1 action permit
switch(configure-filter-ipv4-1001)#quit
switch(config)#interface vlan 10
switch(config-vlanif-10)#igmp group-policy filter-list 1001
switch(config-vlanif-10)#
```

5.3.11igmp require-router-alert

Function

igmp require-router-alert command is used to configure the received IGMP message head to include the Router-Alert Parameters.
no igmp require-router-alert command is used to recover to be the default.

Format

- **igmp require-router-alert**
- **no igmp require-router-alert**

Parameters

None

Default Value

Interface will not check the Router-Alert of IGMP message head and deal with all received IGMP messages including the IGMP message without the Router-Alert.

View

VLANIF Configuration View

Usage Guidelines

After using this command to configure interface to check the Router-Alert, if the received message does not include this Parameters, the IGMP message will be dropped. This command is applied to IGMPv2 and IGMPv3 version.
This Function (only effective for current interface) is similar to the command of require-router-alert (globally effective) and only the configuration view is different. System first uses the interface configuration and then uses the configuration in IGMP Configuration View.

Example

Configure interface to check the Router-Alert.

```
switch(config-vlanif-100)#igmp require-router-alert
switch(config-vlanif-100)#
```

5.3.12 igmp robust-count

Function

igmp robust-count command is used to configure the IGMP querier robust coefficient on interface.

Format

- **igmp robust-count** { *robust* | **default** }

Parameters

Parameters	Description	Value
robust	IGMP robust coefficient	integer, 2~7, unit: time
default	Default value	The global value is inherited..

Default Value

The global value is inherited for the robustness count of the IGMP querier

View

VLANIF Configuration View

Usage Guidelines

IGMP querier is charged with maintaining the IGMP group member relationship of interface and the robust coefficient will influence the timeout interval of group member.
Timeout interval of group member relationship = IGMP general query message sending interval ×robust count + max-response-time
This Function (only effective for current interface) is similar to the command of robust-count (globally effective) and only the configuration view is different. System first uses the interface configuration and then uses the configuration in IGMP Configuration View.

Example

#Configure the IGMP querier robust coefficient on interface.

```
switch(config-vlanif-100)#igmp robust-count 4
switch(config-vlanif-100)#
```

5.3.13 igmp send-router-alert

Function

igmp send-router-alert command is used to configure the sent IGMP message to include the Router-Alert Parameters.
no igmp send-router-alert command is used to configure the sent IGMP message not to include the Router-Alert Parameters.

Format

- **igmp send-router-alert**
- **no igmp send-router-alert**

Parameters

None

Default Value

Include Router-Alert Parameters

View

VLANIF Configuration View

Usage Guidelines

This Function (only effective for current interface) is similar to the command of send-router-alert (globally effective) and only the configuration view is different. System first uses the interface configuration and then uses the configuration in IGMP Configuration View.

Example

#Configure the sent IGMP message to include the Router-Alert Parameters.

```
switch(config-vlanif-100)#igmp send-router-alert
switch(config-vlanif-100)#
```

5.3.14 igmp {start|stop}

Function

igmp {start|stop} command is used to globally enable or disable IGMP function.

Format

- **igmp** { **start** | **stop** }

Parameters

Parameters	Description	Value
start	make effective	-
stop	make ineffective	-

Default Value

Disabled

View

Global Configuration View

Usage Guidelines

This command is the precondition for configuring other IGMP Parameters. Only enabling global IGMP function, other configuration can be effective.

Example

Enable or Disable IGMP function.

```
switch(config)#igmp start
```

```
switch(config)#
switch(config)#igmp stop
```

5.3.15 igmp static-group

Function

igmp static-group command is used to create the IGMP static multicast group on interface.
no igmp static-group command is used to delete the created IGMP static multicast group on interface.

Format

- **igmp static-group** *group-address*
- **no igmp static-group** *group-address*

Parameters

Parameters	Description	Value
group-address	multicast group address	224.0.0.0~239.255.255.255

Default Value

No any static multicast group on interface

View

VLANIF Configuration View

Usage Guidelines

None

Example

Create the IGMP static multicast group on interface.

```
switch(config-vlanif-100)#igmp static-group 224.1.1.1
switch(config-vlanif-100)#
```

5.3.16 igmp static-group egress-port

Function

igmp static-group egress-port command is used to create IGMP static multicast group on interface and designate the egress port.
no igmp static-group egress-port command is used to delete the configured IGMP static multicast group on interface and the designated egress port.

Format

- **igmp static-group** *group-address* **egress-port** { **10gigaethernet** | **100gigaethernet** } *interface-number*

- **igmp static-group** *group-address* **egress-port eth-trunk** *trunk-number*
- **no igmp static-group** *group-address* **egress-port** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **no igmp static-group** *group-address* **egress-port eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
group-address	multicast group address	224.0.0.0~239.255.255.255
interface-number	egress port number	integer, <1~1>/<0~2>/<1~52>
trunk-number	Specifies the egress port of the multicast data forwarding.	It is an integer ranging from 1 to 32.

Default Value

No static multicast group

View

VLANIF Configuration View

Usage Guidelines

After using this command to configure the static multicast group on interface, the created table does not have timer of device and device will think that the interface is always connected with the group member and it will forward the eligible multicast packet to the network segment of the interface. At the same time, device will delete the static group configuration by manually to realize that the receiver will not receive multicast data any more.

Example

Create IGMP static multicast group on interface and designate the egress port.

```
switch(config-vlanif-100)#igmp static-group 224.1.1.1 egress-port 10gigaethernet 1/0/1
switch(config-vlanif-100)#
```

5.3.17 igmp static-group source

Function

igmp static-group source command is used to create the IGMP static group and designate multicast source address.
no igmp static-group source command is used to delete the IGMP static group and the multicast source address.

Format

- **igmp static-group** *group-address* **source** *source-address*
- **no igmp static-group** *group-address* **source** *source-address*

Parameters

Parameters	Description	Value
group-address	multicast group address	224.0.0.0~239.255.255.255
source-address	multicast source	dotted decimal

Default Value

No static multicast group

View

VLANIF Configuration View

Usage Guidelines

None

Example

create the IGMP static group and designate multicast source address.

```
switch(config-vlanif-100)#igmp static-group 224.1.1.1 source 10.18.11.1
switch(config-vlanif-100)#
```

5.3.18 igmp static-group source egress-port

Function

igmp static-group source egress-port command is used to create the IGMP static group and designate the egress port and multicast source address.
no igmp static-group source egress-port command is used to delete the IGMP static group and the egress port and multicast source address.

Format

- **igmp static-group** *group-address* **source** *source-address* **egress-port** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **igmp static-group** *group-address* **source** *source-address* **egress-port eth-trunk** *trunk-number*
- **no igmp static-group** *group-address* **source** *source-address* **egress-port** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **no igmp static-group** *group-address* **source** *source-address* **egress-port eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
group-address	multicast group address	224.0.0.0~239.255.255.255
source-address	multicast source	dotted decimal
interface-number	egress interfacenumber	integer, <1~1>/<0~2>/<1~52>

Parameters	Description	Value
trunk-number	Specifies the output port number.	It is an integer ranging from 1~32

Default Value

No static multicast group

View

VLANIF Configuration View

Usage Guidelines

After using this command to configure the static multicast group on interface, the created table does not have timer of device and device will think that the interface is always connected with the group member and it will forward the eligible multicast packet to the network segment of the interface. At the same time, device will delete the static group configuration by manually to realize that the receiver will not receive multicast data any more.

Example

create the IGMP static group and designate the egress port and multicast source address.

```
switch(config-vlanif-100)#igmp static-group 224.1.1.1 source 10.18.11.1 egress-port 10gigaethernet 1/0/1
switch(config-vlanif-100)#
```

5.3.19 igmp ssm-mapping {enable|disable}

Function

igmp ssm-mapping {enable|disable} command is used to enable or disable SSM mapping function on interface.

Format

- **igmp ssm-mapping** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	make effective	-
disable	make ineffective	-

Default Value

Disable

View

VLANIF Configuration View

Usage Guidelines

Before using this comman, please first use command of igmp {enable|disable}.
After enabling SSM mapping function on interface, the configured SSM source/group address mapping table can be effective and only be effective for received v1 and v2 joining and will change the v1v2 joining IGMP group to be the destigated source joining.

Example

#Enable SSM mapping function on interface.

```
switch((config-vlanif-1)#igmp enable
switch((config-vlanif-1)#igmp ssm-mapping enable
switch((config-vlanif-1)#
```

5.3.20 igmp ssm-mapping filter-list source-address

Function

The **igmp ssm-mapping filter-list source-address** command is used to configure the SSM mapping relationship table of multicast VLAN.
The **no igmp ssm-mapping filter-list source-addresss** command deletes an SSM mapping entry in a multicast VLAN.

Format

- **igmp ssm-mapping filter-list** *acl-number* **source-address** *src-ip-address*
- **no igmp ssm-mapping filter-list** *acl-number* **source-address** *src-ip-address*

Parameters

Parameters	Description	Value
acl-number	ACL number	integer, 1001~2000
src-ip-address	the source IP address to be mapped	dotted decimal

Default Value

None

View

IGMP Configuration View

Usage Guidelines

Before using this command, please first create IPv4 AC.

Example

configure the SSM mapping relationship table of multicast VLAN.

```
switch(config)#filter-list 1001
switch(configure-filter-ipv4-1001)#quit
switch(config)#igmp start
switch(config)#igmp
switch(config-igmp)#
switch(config-igmp)#igmp ssm-mapping filter-list 1001 source-address 1.1.1.1
switch(config-igmp)#
```

5.3.21 igmp timer query

Function

igmp timer query command is used to configure the sending interval of IGMP general group query message on interface.

Format

- **igmp timer query** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	the sending interval of IGMP general group query message	integer, 2~10000, unit: second
default	Default Value	The default value is the global dynamic value.

Default Value

The default value is the global dynamic value.

View

VLANIF Configuration View

Usage Guidelines

This Function (only effective for current interface) is similar to the command of timer query (globally effective) and only the configuration view is different. System first uses the interface configuration and then uses the configuration in IGMP Configuration View.

Example

Configure the sending interval of IGMP general group query message on interface.

```
switch(config-vlanif-100)#igmp timer query 100
```

```
switch(config-vlanif-100)#
```

5.3.22 igmp version

Function

igmp version command is used to configure the running IGMP version of interface.

Format

- **igmp version** { **v1** | **v2** | **v3** | **default** }

Parameters

Parameters	Description	Value
v1	IGMPv1	-
v2	IGMPv2	-
v3	IGMPv3	-
default	Default Value	IGMPv2

Default Value

IGMPv2

View

VLANIF Configuration View

Usage Guidelines

All device interfaces should support the same IGMP version and it cannot switch automatically among all IGMP versions.

Example

#configure the running IGMP version of interface.

```
switch(config-vlanif-100)#igmp version v1
switch(config-vlanif-100)#
```

5.3.23 lastmember-queryinterval

Function

lastmember-queryinterval command is used to globally configure the interval of the IGMP last group member query message sent out when the IGMP querier receives the IGMP leaving message sent by the host.

Format

- **lastmember-queryinterval** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	the interval of the IGMP last group member query message sent out	integer, 1~5, unit: second
default	Default Value	1s

Default Value

1s

View

IGMP Configuration View

Usage Guidelines

This Function (globally effective) is similar to the command of igmp lastmember-queryinterval (only effective for current interface) and only the configuration view is different. System first uses the interface configuration and then uses the configuration in IGMP Configuration View.

Example

Configure the interval of the IGMP last group member query message sent out when the IGMP querier receives the IGMP leaving message sent by the host.

```
switch(config-igmp)#lastmember-queryinterval 2
switch(config-igmp)#
```

5.3.24 limit

Function

limit command is used to configure the maximum number of IGMP table created by system.

Format

- **limit** { *number* | **default**

Parameters

Parameters	Description	Value
number	the maximum number of IGMP table created by system	integer, 1-1024
default	Default Value	1024

Default Value

1024

View

IGMP Configuration View

Usage Guidelines

When the IGMP table item number reach the limit number, it will not create new IGMP table item. If it needs to add new multicast group, it is recommended to delete some useless item or modify the limit number or join in static multicast group.

Example

#Configure the maximum number of IGMP table created by system.

```
switch(config-igmp)#limit 1000
switch(config-igmp)#
```

5.3.25 max-response-time

Function

max-response-time command is used to globaaly configure the maximum response interval of IGMP query message.

Format

- **max-response-time** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	the maximum response interval of IGMP query message	integer, 1~25, unit: second
default	Default Value	10s

Default Value

10s

View

IGMP Configuration View

Usage Guidelines

This Function (globally effective) is similar to the command of igmp max-response-time (only effective for current interface) and only the configuration view is different. System first uses the interface configuration and then uses the configuration in IGMP Configuration View.

Example

#Configure the maximum response interval of IGMP query message.

```
switch(config-igmp)#max-response-time 15
```

```
switch(config-igmp)#
```

5.3.26 no igmp group vlan

Function

no igmp group vlan command is used to delete the dynamic multicast group records related with the group address of VLAN interface.
no igmp group vlan all command is used to delete all dynamic multicast group records.

Format

- **no igmp group vlan** *vlan-id*
- **no igmp group vlan** *vlan-id group-address*
- **no igmp group all**

Parameters

Parameters	Description	Value
vlan-id	VLAN ID of dynamic multicast group	integer, 1~4094
group-address	IP address of dynamic multicast group	224.0.0.0~239.255.255.255
all	all dynamic multicast group records	-

Default Value

None

View

IGMP Configuration View

Usage Guidelines

None

Example

#Delete the dynamic multicast group records related with the group address of VLAN interface.

```
switch(config-igmp)#no igmp group vlan 100
switch(config-igmp)#
```

5.3.27 no igmp group vlan source

Function

no igmp group vlan source command is used to delete the dynamic multicast group source related with the group address and specific VLAN interface.

Format

- **no igmp group vlan** *vlan-id group-address* **source** *source-address*
- **no igmp group vlan** *vlan-id group-address* **source all**

Parameters

Parameters	Description	Value
vlan-id	VLAN ID	integer, 1~4094
group-address	IP address of dynamic multicast group	224.0.0.0~239.255.255.255
source-address	multicast source address	dotted decimal
all	all multicast source	-

Default Value

None

View

IGMP Configuration View

Usage Guidelines

None

Example

#Delete the dynamic multicast group source related with the group address and specific VLAN interface.

```
switch(config-igmp)#no igmp group vlan 100 224.1.1.0 source 10.18.2.12
switch(config-igmp)#
```

5.3.28 no igmp group vlan source egress-port

Function

no igmp group vlan source egress-port command is used to delete the dynamic egress port of specific VLAN interface, group address and multicast source.

Format

- **no igmp group vlan** *vlan-id group-address* **source** *source-address* **egress-port** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **no igmp group vlan** *vlan-id group-address* **source** *source-address* **egress-port all**

Parameters

Parameters	Description	Value
vlan-id	VLAN ID	integer, 1~4094

Parameters	Description	Value
group-address	IP address of dynamic multicast group	224.0.0.0~239.255.255.255
source-address	multicast source address	dotted decimal
interface-number	egress port number	integer, <1~1>/<0~2>/<1~52>
all	all egress ports	-

Default Value

None

View

IGMP Configuration View

Usage Guidelines

None

Example

Delete the dynamic egress port of specific VLAN interface, group address and multicast source.

```
switch(config-igmp)#no igmp group vlan 1 255 1.1.1 source 10.18.2.12 egress-port 10gigaethernet 1/0/1
switch(config-igmp)#
```

5.3.29 require-router-alert

Function

require-router-alert command is used to globally configure the received IGMP message head to include the Router-Alert Parameters.
no equire-router-alert command is used to recover to be the default.

Format

- **require-router-alert**
- **no require-router-alert**

Parameters

None

Default Value

Device will not check the Router-Alert of IGMP message head and deal with all received IGMP messages including the IGMP message without the Router-Alert.

View

IGMP Configuration View

Usage Guidelines

After using this command to check the Router-Alert, if the received message does not include this Parameters, the IGMP message will be dropped. This command is applied to IGMPv2 and IGMPv3 version.
This Function (globally effective) is similar to the command of igmp require-router-alert (only effective for current interface) and only the configuration view is different. System first uses the interface configuration and then uses the configuration in IGMP Configuration View.

Example

#Configure the received IGMP message head to include the Router-Alert Parameters.

```
switch(config-igmp)#require-router-alert
switch(config-igmp)#
```

5.3.30 robust-count

Function

robust-count command is used to globally configure the IGMP querier robust coefficient.

Format

- **robust-count** { *robust* | **default** }

Parameters

Parameters	Description	Value
robust	the IGMP querier robust coefficient	integer, 2~7, unit: times
default	Default Value	2times

Default Value

2

View

IGMP Configuration View

Usage Guidelines

IGMP querier robust coefficient is defined by the following two values.

- the times of sending general group query when querier starts
- the times of sending specific group query message after querier receives leaving message

This Function (globally effective) is similar to the command of igmp robust-count (only effective for current interface) and only the configuration view is different. System first uses the interface configuration and then uses the configuration in IGMP Configuration View.

Example

#Configure the IGMP querier robust coefficient.

```
switch(config-igmp)#robust-count 3
switch(config-igmp)#
```

5.3.31 send-router-alert

Function

send-router-alert command is used to globally configure the sent IGMP message to include the Router-Alert Parameters.
no send-router-alert command is used to globally configure the sent IGMP message not to include the Router-Alert Parameters.

Format

- **send-router-alert**
- **no send-router-alert**

Parameters

None

Default Value

None

View

IGMP Configuration View

Usage Guidelines

This command is usually used with require-router-alert.
This Function (globally effective) is similar to the command of igmp send-router-alert (only effective for current interface) and only the configuration view is different. System first uses the interface configuration and then uses the configuration in IGMP Configuration View.

Example

#Configure the sent IGMP message to include the Router-Alert Parameters.

```
switch(config-igmp)#send-router-alert
switch(config-igmp)#
```

5.3.32 show igmp

Function

show igmp command is used to display IGMP global resource information.

Format

- **show igmp**

Parameters

None

Default Value

None

View

Common User View, Privilege User View, Global Configuration View, VLANIF Configuration View, IGMP Configuration View

Usage Guidelines

None

Example

#Display IGMP global resource information.

```
switch#show igmp
  Version                    :IGMP_VB3.00.00.00
  IGMP is Started
  Global Interface Maximum: 64
  Global Group Maximum: 2000
  Global Source Maximun: 2000
  Global Egress Maximum: 2000
  switch#
```

5.3.33 show igmp config

Function

show igmp config command is used to display IGMP configuration information.

Format

- **show igmp config**

Parameters

None

Default Value

None

View

Common User View, Privilege User View, Global Configuration View, VLANIF Configuration View, IGMP Configuration View

Usage Guidelines

None

Example

Display IGMP configuration information.

```
switch#show igmp config
igmp start
igmp

Interface vlan-1
 igmp enable
 igmp version v1
 igmp max-response-time 100
 igmp fast-leave enable
 igmp require-router-alert
 igmp limit 100

switch#
```

5.3.34 show igmp egress-port

Function

show igmp egress-port command is used to display IGMP egress interface information.

Format

- **show igmp egress-port** { **static** | **dynamic** | **all** } [**vlan** *vlan-id*]
- **show igmp egress-port** { **static** | **dynamic** | **all** } **vlan** *vlan-id* **group** *group-address*
- **show igmp egress-port** { **static** | **dynamic** | **all** } **vlan** *vlan-id* **group** *group-address* **source** *source-address*

Parameters

Parameters	Description	Value
vlan-id	VLAN ID	Integer, 1~4094
group-address	Multicast group address	Dotted deicmal, 224.0.0.0~239.255.255.255
source-address	Multicast source	Dotted deicmal
static	Delete static multicast group	-
dynamic	Delete dynamic multicast group	-
all	Delete all multicast groups	-

Default Value

None

View

Common User View, Privilege User View, Global Configuration View, VLANIF Configuration View, IGMP Configuration View

Usage Guidelines

None

Example

#Display IGMP egress interface information.

```
switch#show igmp egress-port all

 Interface        Group-Address    Source-Address   Egress-Port                Status
 vlan-1           233.1.1.1        0.0.0.0          10ge-1/0/2                 static
switch#
```

5.3.35 show igmp group

Function

show igmp group command is used to display IGMP group information.

Format

- **show igmp group** { **static** | **dynamic** | **all** } [**vlan** *vlan-id*]

Parameters

Parameters	Description	Value
vlan-id	VLAN ID	Integer, 1~4094
static	Display static multicast group	-
dynamic	Display dynamic multicast group	-
all	Display all multicast groups	-

Default Value

None

View

Common User View, Privilege User View, Global Configuration View, VLANIF Configuration View, IGMP Configuration View

Usage Guidelines

None

Example

#Display IGMP group information.

```
switch#show igmp group all

 Vpn Instance:N/A
 Interface:vlan-1
  Group Address:233.1.1.1
  Last Reporter Address:0.0.0.0
  Uptime:2000/01/07    18:18:45
  Expiry Time:0 s
  Exclude Mode Expiry Time:0 s
  V1 Host Timer:0 s
  V2 Host Timer:0 s
  Filter Mode:include
  Group Status:static
switch#
```

5.3.36 show igmp interface

Function

show igmp interface command is used to display IGMP interface information.

Format

- **show igmp interface**
- **show igmp interface vlan** *vlan-id*

Parameters

Parameters	Description	Value
vlan-id	VLAN ID	Integer, 1~4094

Default Value

None

View

Common User View, Privilege User View, Global Configuration View, VLANIF Configuration View, IGMP Configuration View

Usage Guidelines

None

Example

View the IGMP interface information.

```
switch#show igmp interface

 Interface        Querier-address     Version Fast-leave      Querier-remain
 vlan-1           0.0.0.0             v2      disable         97

switch#
```

View the IGMP information of VLAN1.

```
switch#show igmp interface vlan 1
Interface vlan-1
IGMP VPN Instance: N/A
   IGMP Status: enable
   Require-router-alert: disable
   Send-router-alert: enable
   Timer Query: 125 s
   Robust-count: 2
   Max Response Time: 10 s
   Timer Other Querier Present: 255 s
   Last Member Query Interval: 1 s
   Version: v2
   Fast-leave: disable
   Querier Uptime: 453 s
   Wrong Version Querier: 0
   Joins: 0
   Groups: 1
   Last Listener Query Count: 2
   Startup Query Count: 0
   Startup Query Interval: 31 s
   Query Remain: 76 s
   Querier Address: 0.0.0.0
   SSM Mapping: disable
   IGMP Limit: 2000
switch#
```

5.3.37 show igmp source

Function

show igmp source command is used to display IGMP source information.

Format

- **show igmp source** { **static** | **dynamic** | **all** } [**vlan** *vlan-id*]
- **show igmp source** { **static** | **dynamic** | **all** } **vlan** *vlan-id* **group** *group-address*

Parameters

Parameters	Description	Value
vlan-id	VLAN ID	Integer, 1~4094
group-address	IGMP group address	Dotted decimal, 224.0.0.0~239.255.255.255
static	Display static multicast group	-
dynamic	Display dynamic multicast group	-
all	Display all multicast groups	-

Default Value

None

View

Common User View, Privilege User View, Global Configuration View, VLANIF Configuration View, IGMP Configuration View

Usage Guidelines

None

Example

Display IGMP source information.

```
switch#show igmp source all

 Interface        Group-Address    Source-Address  Expiry-Time      Mode      Status
 vlan-1           233.1.1.1        0.0.0.0         0                include static

switch#
```

5.3.38 show igmp ssm-mapping

Function

show igmp ssm-mapping command is used to display the IGMP group information with mapping rule configured by ssm-mapping.

Format

- **show igmp ssm-mapping**

Parameters

None

Default Value

None

View

Common User View, Privilege User View, Global Configuration View, VLANIF Configuration View, IGMP Configuration View

Usage Guidelines

None

Example

#Display the IGMP group information with mapping rule configured by ssm-mapping.

```
switch(config-igmp)#show igmp ssm-mapping
  Vpn-Instance                    Filter-listSource Address
  Public                          1001        1.1.1.1
switch(config-igmp)#
```

5.3.39 timer other-querier-present

Function

timer other-querier-present command is used to globally configure the timeout interval of other IGMP queriers.

Format

- **timer other-querier-present** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	the timeout interval of other IGMP queriers	integer, 1~65535, unit: second
default	Default Value	255s

Default Value

255s

View

IGMP Configuration View

Usage Guidelines

the timeout interval of other IGMP querier = robust × IGMP general group query message sending interval +（1/2）× the maximum response interval of query message
This command is applied to IGMPv2 and IGMPv3. This Function (globally effective) is similar to the command of igmp timer other-querier-present (only effective for current interface) and only the configuration view is different. System first uses the interface configuration and then uses the configuration in IGMP Configuration View.

Warning: If the timeout interval of other IGMP querier is less than the IGMP general group query message sending interval, it will result in repeated change of querier in network. User shold be careful to configure.

Example

#Configure the timeout interval of other IGMP queriers.

```
switch(config-igmp)#timer other-querier-present 100
switch(config-igmp)#
```

5.3.40 timer query

Function

timer query command is used to globally configure the sending interval of IGMP general group query message.

Format

- **timer query** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	the sending interval of IGMP general group query message	integer, 1~65535, unit: second
default	Default Value	125s

Default Value

125s

View

IGMP Configuration View

Usage Guidelines

This Function (globally effective) is similar to the command of igmp timer query (only effective for current interface) and only the configuration view is different. System first uses the interface configuration and then uses the configuration in IGMP Configuration View.

Example

#Configure the sending interval of IGMP general group query message.

```
switch(config-igmp)#timer query 100
switch(config-igmp)#
```

5.4 PIMv4 Configuration Command

5.4.1 assert-holdtime

Function

The **assert-holdtime** command sets the Assert state hold time for all the PIM interfaces on the switch.

Format

- **assert-holdtime** { *time* | **default** }

Parameters

Parameters	Description	Value
time	Specifies the Assert state hold time for all the PIM interfaces on the switch.	It is an integer ranging from 7 to 65535 (unit: s).
default	Restores the Assert state hold time for all the PIM interfaces on the switch to the default value.	180s

Default Value

180s

View

PIM configuration view

Usage Guidelines

None

Example

Set the Assert state hold time for all the PIM interfaces on the switch to 30 seconds.

```
switch(config-pim)#assert-holdtime 30
switch(config-pim)#
```

5.4.2 accept-unknown-rp {enable|disable}

Function

The **accept-unknown-rp enable** command enables processing the join / prune messages with unknown RPs.
The **accept-unknown-rp disable** command disables processing the join / prune messages with unknown RPs.

Format

- **accept-unkown-rp enable**
- **accept-unkown-rp disable**

Parameters

None

Default Value

The processing of the join / prune messages with unknown RPs is disabled.

View

PIM configuration view

Usage Guidelines

None

Example

Enable processing the join / prune messages with unknown RPs.

```
switch(config)#ip multicast-routing
switch(config)#pim
switch(config-pim)#accept-unknown-rp enable
switch(config-pim)#
```

5.4.3 c-bsr admin-scope {enable|disable}

Function

c-bsr admin-scope {enable|disable} command can be used to enable or disable BSR management domain function configured in the PIM-SM domain.

Format

- **c-bsr admin-scope** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	enable BSR management domain function configured in the PIM-SM domain	-

Parameters	Description	Value
disable	disable BSR management domain function configured in the PIM-SM domain	-

Default Value

Disable

View

PIM Configuration View

Usage Guidelines

BSR management domain is corresponding with some multicast group. The prefix of management domain is 239.0.0.0. That is to say, the range of multicast group address is in the 239.0.0.0/8 network segment.

Example

Enable BSR management domain function configured in the PIM-SM domain.

```
switch(config)#ip multicast-routing
switch(config)#pim
switch(config-pim)#c-bsr admin-scope enable
switch(config-pim)#
```

5.4.4 c-bsr send-interval

Function

The **c-bsr send-interva**l command sets the interval at which the BSR sends Bootstrap packets.

Format

- **c-bsr send-interval** { *time-interval* | **default** }

Parameters

Parameters	Description	Value
time-interval	Specifies the interval at which the BSR continuously sends Bootstrap packets.	It is an integer ranging from 1 to 107374177 (unit: s).
default	Restores the interval at which the BSR continuously sends Bootstrap packets to the default value.	60

Default Value

60s

View

PIM configuration view

Usage Guidelines

None

Example

Set the interval at which the BSR continuously sends Bootstrap packets to 30 seconds.

```
switch(config-pim)#c-bsr send-interval 30
switch(config-pim)#
```

5.4.5 c-rp hold-time

Function

The **c-rp hold-time** command sets the timeout period during which a BSR waits for Advertisement packets sent from the C-RP.

Format

- **c-rp hold-time** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	Specifies the timeout period during which a BSR waits for Advertisement packets sent from the C-RP.	It is an integer ranging from 1 to 65535 (unit: s).
default	Uses the default value.	150s

Default Value

The timeout period during which a BSR waits for Advertisement packets sent from the C-RP is 150s.

View

PIM configuration view

Usage Guidelines

The hold-time is carried in the Advertisement packet sent from the C-RP to the BSR. After BSR receives the packets, the timer starts and the time is set by this command. If the subsequent Advertisement packets from the C-RP are not received after the time is out, BSR ascertains that the C-RP fails or is unreachable. In this case, BSR will not summarize the information to the RP-set and then send to the devices in the domain.

Example

Set the timeout period during which a BSR waits for Advertisement packets sent from the C-RP.

```
switch(config)#ip multicast-routing
switch(config)#pim
switch(config-pim)#c-rp hold-time 100
switch(config-pim)#
```

5.4.6 c-rp send-interval

Function

The **c-rp send-interval** command sets the interval of the periodic Advertisement packet periodic transmission by the C-RP.

Format

- **c-rp send-interval** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	Specifies the interval of the Advertisement packet transmission by the C-RP.	It is an integer ranging from 1 to 65535 (unit: s).
default	Uses the default value.	60s

Default Value

The interval of the Advertisement packet transmission by the C-RP is 60s.

View

PIM configuration view

Usage Guidelines

All the C-RPs within the PIM-SM domain transmit the Advertisement packets carrying their own parameters to the BSR periodically. Then the BSR summarizes the C-RP information into an RP set and sends it to all the devices within the domain. You can use this command to set the interval of the Advertisement packet transmission to BSR by the C-RP.

Example

Set the interval of the periodic Advertisement packet transmission by the C-RP.

```
switch(config)#ip multicast-routing
switch(config)#pim
switch(config-pim)#c-rp send-interval 30
switch(config-pim)#
```

5.4.7 ip multicast-routing

Function

ip multicast-routing command can be used to start PIM protocol.
no ip multicast-routing command can be used to stop PIM protocol.

Format

- **ip multicast-routing**
- **no ip multicast-routing**

Parameters

None

Default Value

no PIM protocol operated

View

Global Configuration View

Usage Guidelines

None

Example

#Enable the multicast routing protocol.

```
switch(config)#ip multicast-routing
switch(config)#
```

5.4.8 ip pim {pim-sm|pim-dm}

Function

ip pim-sm command can be used to enable PIM-SM at interface.
no ip pim-sm command can be used to disable PIM-SM at interface.
ip pim-dm command can be used to enable PIM-DM at interface.
no ip pim-dm command can be used to disable PIM-DM at interface.

Format

- **ip pim-sm**
- **no ip pim-sm**
- **ip pim-dm**
- **no ip pim-dm**

Parameters

None

Default Value

disabled

View

VLANIF Configuration View

Usage Guidelines

Device is able to establish PIM neighbor with neighbor device and to execute protocol message from PIM neighbor only when the PIM protocol is global started and PIM-SM is interface enabled.

Warning: Please make sure the global PIM has been started before configuring IP PIM, i.e., 'ip multicast-routing' is enabled.

Example

Enable PIM-SM at interface.

```
switch(config)#int vlan 100
switch(config-vlanif-100)#ip pim-sm
switch(config-vlanif-100)#
```

5.4.9 ip pim bsr-boundary group

Function

The **ip pim bsr-boundary** command adds the boundary interface to a management domain.
The **no ip pim bsr-boundary** command deletes the boundary interface of the management domain.

Format

- **ip pim bsr-boundary group** *group-ip-address/M*
- **ip pim bsr-boundary group default**
- **no ip pim bsr-boundary group** *group-ip-address/M*
- **no ip pim bsr-boundary group default**

Parameters

Parameters	Description	Value
group-ip-address	Specifies the group IP address	The value is in dotted decimal notation. The value ranges from 224.0.0.0 to 239.255.255.255.
M	Specifies the mask length.	It is an integer ranging from 4 to 32.

Default Value

224.0.0.0/4

View

VLANIF configuration view

Usage Guidelines

Configure the boundary router of PIM on the interface, so that one large PIM network can be devided into multiple PIM domains. Each BSR serves the local PIM-SM domain only. Bootstrap packets cannot pass through the BSR boundary, but other multicast packets can.
The boundary router of the PIM domain mainly generates RP entries and forbids the BSR message transmission. Boundary routers need not be configured.

Example

Add a boundary interface to the management domain.

```
switch(config-vlanif-100)#ip pim bsr-boundary group default
switch(config-vlanif-100)#
```

5.4.10 ip pim c-bsr

Function

ip pim c-bsr command can be used to configure candidate bootstrap router.

Format

- **ip pim c-bsr group** *group-ip-address/mask-len* **hash-length** *hash-length* **priority** *priority*
- **ip pim c-bsr group default**
- **no ip pim c-bsr group** *group-ip-address/mask-len*
- **no ip pim c-bsr group default**

Parameters

Parameters	Description	Value
group-ip-address/mask-len	Multicast group address with range of 225.0.0.1-239.255.255.255 and mask as 1-32	Dotted decimal
hash-length	Hash length for calculating best RP when there is more than one RPs within a multicast group	Integer form with range of 0-32
priority	Priority. When there is more than one candidate RPs, the one with higher priority will be voted.	Integer form with range of 0-255

Default Value

None

View

VLANIF Configuration View

Usage Guidelines

None

Example

Configure candidate bootstrap router.

```
switch(config-vlanif-1)#ip pim c-bsr group 225.0.0.0/24 hash-length 32 priority 1
switch(config-vlanif-1)#
```

5.4.11ip pim c-rp group priority

Function

ip pim c-rp group priority command can be used to configure the router interface as candidate RP.
no ip pimc-rp command can be used to delete C-RP configuration.

Format

- **ip pim c-rp group** *group-ip-address/mask-length* **priority** *priority*
- **ip pim c-rp group default**
- **no ip pim c-rp** *group-ip-address/mask-length*
- **no ip pim c-rp group default**

Parameters

Parameters	Description	Value
group-ip-address	Address range of CRP service group	Dotted decimal
mask-length	Address mask length of CRP service group	Integer form with range of 1-32
priority	CRP priority default: 192	Integer form with range of 0-255

Default Value

None

View

VLANIF Configuration View

Usage Guidelines

None

Example

Configure the router interface as candidate RP.

```
switch(config-vlanif-1)#ip pim c-rp group 225.1.1.0/24 priority 5
switch(config-vlanif-1)#
```

5.4.12 ip pim dr-priority

Function

ip pim dr-priority command can be used to configure PIM interface voting for DR priority.

Format

- **ip pim dr-priority** { *priority* | **default** }

Parameters

Parameters	Description	Value
priority	Indicates that the PIM interface voting for DR priority	Integer form with range of 0~4294967294
default	default priority	Integer form with default 1

Default Value

In default, the priority of PIM interface voting DR is 1.

View

VLANIF Configuration View

Usage Guidelines

When the interface with IP address configured has PIM enabled, the command is used for configuration of PIM DR priority. The priority is for DR vote among PIM neighbors at a same interface (DR with higher priority if priorities are not the same, and DR with larger IP address if priorities are the same will be voted).

Example

#Configure PIM interface voting for DR priority.

```
switch(config-vlanif-100)#ip pim dr-priority 100
switch(config-vlanif-100)#
```

5.4.13 ip pim graft retry-time

Function

The **ip pim graft retry-time** command configures the interval of re-transmitting graft messages.

Format

- **ip pim graft retry-time** { *graft-interval* | **default** }

Parameters

Parameters	Description	Value
graft-interval	Specifies the interval of re-transmitting graft messages.	It is an integer ranging from 1 to 65535 (unit: s).
default	Uses the default interval of re-transmitting graft messages.	It is an integer. The value is value 3s.

Default Value

3s

View

VLANIF configuration view

Usage Guidelines

In PIM-DM mode, the switch sends a grafting message and waits for the confirmation from the upstream when a member joins a group that has been pruned. If no confirmation is received during the command execution, the switch will retransmit the grafting message until it receives the confirmation from the upstream.

Example

Configure the interval of re-transmitting graft messages to 10s.

```
switch(config-vlanif-1)#no ip pim-sm
switch(config-vlanif-1)#ip pim-dm
switch(config-vlanif-1)#ip pim graft retry-time 10
switch(config-vlanif-1)#
```

5.4.14 ip pim hello-interval

Function

The **ip pim hello-interval** command can be used to configure time interval of PIM interface sending Hello message.

Format

- **ip pim hello-interval** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	Time interval of PIM interface sending Hello message	Integer form with range of 0~65535 and unit as seconds
default	default time interval	Integer form with default 30 seconds.

Default Value

30 seconds

View

VLANIF Configuration View

Usage Guidelines

When the interface with IP address configured has been PIM enabled, the command can be utilized for configuration of sending Hello message frequency at the interface.

Example

#Configure time interval of PIM interface sending Hello message.

```
switch(config-vlanif-100)#ip pim hello-interval 60
switch(config-vlanif-100)#
```

5.4.15 ip pim hello-option holdtime

Function

The **ip pim hello-option holdtime** command configures the hold-off time during which a PIM interface waits for Hello packets sent from the PIM neighbors.

Format

- **ip pim hello-option holdtime** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	Sepcifies the hold-off time during which a PIM interface waits for Hello packets sent from the PIM neighbors.	It is an integer ranging from 1 to 65535 (unit: s).
default	Uses the default hold-off time during which a PIM interface waits for Hello packets sent from the PIM neighbors.	105s

Default Value

105s

View

VLANIF configuration view

Usage Guidelines

In the PIM network, the equipment will trigger the timer after receiving the Hello packets sent from the PIM neighbors. The time is set to the hold-time carried in the packet. If the equipment does not receive the Hello packets senf from a neighbor after the time expired, the neighbor fails or becomes unreachable.
You can set the hold time using this command to adjust the hold time of Hello packets. The hold time should be larger than the Hello packet transmission interval.

Example

Set the hold-off time during which the VLANIF100 interface waits for Hello packets sent from the PIM neighbors to 60s.

```
switch(config-vlanif-100)#ip pim hello-option holdtime 60
switch(config-vlanif-100)#
```

5.4.16 ip pim hello-option neighbor-tracking

Function

The **ip pim hello-option neighbor-tracking** command enables or disables the neighbor tracking.

Format

- **ip pim hello-option neighbor-tracking** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the neighbor tracking.	-
disable	Disables the neighbor tracking.	-

Default Value

The neighbor tracking is disabled.

View

VLANIF configuration view

Usage Guidelines

When sending a Hello message, the device generates a Generation ID carred in the message. Generally, the generation ID will not change. The generation ID changes only if the device status changes and a new generation ID is generated. After receiving the Hello message, the neighbor device finds that the Generation ID changes, and immediately sends the join message to the device to refresh the neighbor relationship. Normally, if multiple devices in the shared network segment are ready to send join requests to one upstream device, the snooping mechanism will be used to suppress the number of same join messages, that is, a device will not send join messages to the upstream PIM neighbors after snooping join messages from other devices. In this case, the upstream neighbor fails to refresh the neighbor relationship with each downstream device due to the Generation ID change.

This command can be used to enable the neighbor tracking. After snooping the join messages sent by other devices, the device will not suppress sending join messages to the same upstream PIM neighbor.

Before running this command, run the "ip multicast" command in the the public network to enable the multicast routing function.

This function only takes effect for the PIM-SM network.

Only if this command is run for all the devices in the shared network segment can neighbor tracking be realized.

Example

Enable the neighbor tracking.

```
switch(config-vlanif-100)#ip pim hello-option neighbor-tracking enable
switch(config-vlanif-100)#
```

5.4.17 ip pim hello-option override-interval

Function

The **ip pim hello-option override-interval** command configures the interval of rejecting pruning in the Hello packets sent from an interface.

Format

- **ip pim hello-option override-interval** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	Specifies the interval of rejececting pruning in the Hello packets sent from an interface.	It is an integer ranging from 0 to 65535 (unit: ms).
default	Uses the default interval of rejecting pruning in the Hello packets sent from an interface.	2500 ms

Default Value

2500 ms

View

VLANIF configuration view

Usage Guidelines

The Hello packet sent from the switch carries the "lan-delay" (packet transmission delay) and "override-interval" (pruning rejection interval) parameters. The "override-interval" parameter indicates the time when the downstream switch is allowed to reject pruning.
If a switch in the same network segment sends pruning packets to the upstream device, and other switches still need to receive multicast data, they must send pruning rejection packets to the upstream device within the "override-interval" time.
If the "override-interval" values of all the switches on the same link are different, the maximum value will be selected from them based on negotiation.
Lan-delay + override-interval = PPT. After receiving the downstream pruning packet, the switch does not immediately perform pruning but waits for a period of Prune-Pending Timer (PPT), and prunes when the time is out. If the downstream pruning rejection packet is received within the PPT time, the pruning will be cancelled.

Example

Set the interval of rejececting pruning in the Hello packets sent from the VLANIF100 interface to 3000 ms.

```
switch(config-vlanif-100)#ip pim hello-option override-interval 3000
```

```
switch(config-vlanif-100)#
```

5.4.18 ip pim hello-option prune-delay

Function

The **ip pim hello-option prune-delay** command configures the delay time of packet transmission in a shared network in the interface configuration view.

Format

- **ip pim hello-option prune-delay** { *delay-value* | **default** }

Parameters

Parameters	Description	Value
delay-value	Specifies the delay time of packet transmission in a shared network.	It is an integer ranging from 0 to 32767 (unit: ms)
default	Uses the default delay time of packet transmission in a shared network.	500 ms

Default Value

500 ms

View

VLANIF configuration view

Usage Guidelines

The Hello packet sent from the switch carries the "lan-delay" (packet transmission delay) and "override-interval" (pruning rejection interval) parameters. The "lan-delay" parameter indicates the delay time of transmitting packets in the LAN. If the "lan-delay" values of all switches on the same link are different, the maximum value will be selected from them based on negotiation.

If a switch in the same network segment sends pruning packets to the upstream device, and other switches still need to receive multicast data, they must send pruning rejection packets to the upstream device within the "override-interval" time.

Lan-delay + override-interval = PPT. PPT represents the delay after the current switch receives the downstream pruning packet and before the pruning (suppressing the downstream interface forwarding) is performed. If the downstream pruning rejection packet is received within the PPT time, the pruning will be cancelled.

Example

Configure the delay time of packet transmission in a shared network in the interface configuration view.

```
switch(config-vlanif-100)#ip pim hello-option prune-delay 600
switch(config-vlanif-100)#
```

5.4.19 ip pim join-prune holdtime

Function

The **ip pim join-prune holdtime** command configures the hold time of the Join / Prune packets. The switches receiving Join / Prune packets ascertains the hold time of joining or pruning of the downstream interface according to the hold time carried by the packets.

Format

- **ip pim join-prune holdtime** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	Indicates the overwriting interval.	It is an integer ranging from 1 to 65535 (unit: s)
default	Uses the default overwriting interval.	210s

Default Value

The overwriting interval is 210s.

View

VLANIF configuration view

Usage Guidelines

After receiving the Join / Prune packet from the downstream, the switch starts the timer whose time is the hold time carried by the Join / Prune packet. If the switch fails to receive the subsequent Join / Prune packet from the downstream devices after the time is out, and the Join / Prune packet carries the information of joining a multicast group, the downstream interface forwarding of the corresponding multicast group will be suppressed. If the Join / Prune packet carries the pruning information for a multicast group, the downstream interface forwarding of the corresponding multicast group will be restored.

Example

Set the hold time of the Join / Prune packets.

```
switch(config-vlanif-100)#ip pim join-prune holdtime 300
switch(config-vlanif-100)#
```

5.4.20 ip pim join-prune interval

Function

The **ip pim join-prune interval** command configures the interval of periodically sending Join / Prune packets to the upstream devices on a PIM interface.

Format

- **ip pim join-prune interval** { *interval*| **default** }

Parameters

Parameters	Description	Value
interval	Sets the interval of periodically sending Join / Prune packets.	It is an integer ranging from 0 to 2147483647 (unit: s).
default	Uses the default interval of periodically sending Join / Prune packets.	It is an integer. The value is 60s.

Default Value

The interval of periodically sending Join / Prune packets to the upstream devices is 60s on a PIM interface.

View

VLANIF configuration view

Usage Guidelines

After an interface is configured with the IP address and enabled with the PIM function, the ip pim join-prune interval command can set the frequency of periodically sending Join / Prune packets for the interface. The frequency can be modified according to the actual situation.
Generally the parameters need not to be modified.

Warning: Before using the ip-pim-related commands, make sure the global PIM is enabled and the PIM-SM on the corresponding VLAN interface is enabled. That is, the ip multicast-routing is enabled, and the ip pim on the corresponding interface VLAN is enabled.

Example

Configure the interval of periodically sending Join / Prune packets on the VLANIF100 interface to 100s.

```
switch(config-vlanif-100)#ip pim join-prune interval 100
switch(config-vlanif-100)#
```

5.4.21 ip pim state-refresh-capable

Function

ip pim state-refresh-capable enable command can be used to enable PIM-DM state refresh function on the interface.
ip pim state-refresh-capable disable command can be used to disable PIM-DM state refresh function on the interface.

Format

- **ip pim state-refresh-capable enable**
- **ip pim state-refresh-capable disable**

Parameters

None

Default Value

Enable PIM-DM state refresh function.

View

VLANIF Configuration View

Usage Guidelines

PIM-DM state refreshing is realized by periodically sending state refreshing message in the network. After the Switch which is in the pruning state receiving the state refreshing message, it will reset the pruning state timer to avoid the downstream interface recovering to transmit for timeout.
After disabling PIM-DM state refreshing and the pruning timer being timeout, interface will start to transmit multicast data and the downstream Switch which not hope to receive the data will send the prune message. It is periodic repetition and occupy many network resources. Thereby, enabling PIM-DM state refreshing function can optimize the network traffic to some extent.

Example

Disable PIM-DM state refresh function on the interface.

```
switch(config-vlanif-1)#ip pim-sm
switch(config-vlanif-1)#ip pim state-refresh-capable disable
switch(config-vlanif-1)#
```

5.4.22 pim

Function

pim command can be used to create PIM public network instance and access PIM public instance configuration view.
no pim command can be used to delete the PIM public network instance.

Format

- **pim**
- **no pim**

Parameters

None

Default Value

None

View

Global Configuration View

Usage Guidelines

None

Example

Create PIM public network instance and access PIM public instance configuration view.

```
switch(config)#pim
switch(config-pim)#
```

5.4.23 receive-check-neighbor

Function

The **receive-check-neighbor** command enables or disables the neighbor detection when the equipment receives the join / prune / assert packets.

Format

- **receive-check-neighbor** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the neighbor detection when the equipment receives the join / prune / assert packets.	-
disable	Disables the neighbor detection when the equipment receives the join / prune / assert packets.	-

Default Value

The neighbor detection is disabled when the equipment receives the join / prune / assert packets.

View

PIM configuration view

Usage Guidelines

None

Example

Enable the neighbor detection when the equipment receives the join / prune / assert packets.

```
switch(config-pim)#receive-check-neighbor enable
switch(config-pim)#
```

5.4.24 register externsion-checksum

Function

register externsion-checksum command can be used to configure to calculate the checksum only according to the Register message extended information.

Format

- **register externsion-checksum** { **enable** | **disable** }

Parameters

None

Default Value

None

View

PIM Configuration View

Usage Guidelines

None

Example

In public network instance, configure to calculate the checksum only according to the Register message extended information.

```
switch(config-pim)#register externsion-checksum enable
switch(config-pim)#
```

5.4.25 register fragment

Function

register fragment command can be used to enable or disable slicing extened function of PIM-SM register message.

Format

- **register fragment** { **enable** | **disable** }

Parameters

None

Default Value

No register message slicing configured.

View

PIM Configuration View

Usage Guidelines

When the length of multicast packet with the register message is over than the interface MTU, it needs to slice. There art two ways to slice. One is that constructing register message first and then slice the register message and is restructured by the RP. The other way is that first slice the multicast packet and then construct two register messages and is restructured by the receiver. It is recommended to use the second way. This can reduce the RP pressure.
This command is used to control the mechanism of choosing register slice. Using this command, it will use the latter method.

Example

Enable slicing extened function of PIM-SM register message.

```
switch(config)#ip multicast-routing
switch(config)#pim
switch(config-pim)#register fragment enable
switch(config-pim)#
```

5.4.26 register mtu

Function

register mtu command can be used to configure the slicing MTU of PIM-SM register message slicing extension.

Format

- **register mtu** { *mtu-value* | **default**

Parameters

Parameters	Description	Value
mtu-value	the slicing MTU value of PIM-SM register message slicing extension	integer, 750-1600, unit: byte
default	Default Value	1500bytes

Default Value

1500 bytes

View

PIM Configuration View

Usage Guidelines

When the length of multicast packet with the register message is over than the interface MTU, it needs to slice. There art two ways to slice. One is that constructing register message first and then slice the register message and is restructured by the RP. The other way is that first slice the multicast packet and then construct two register messages and is restructured by the receiver. It is recommended to use the second way. This can reduce the RP pressure.
Because the link MTU of network is not clear, please use this command to control the size of register message to avoid slicing once again.

Example

Configure the slicing MTU of PIM-SM register message slicing extension.

```
switch(config)#ip multicast-routing
switch(config)#pim
switch(config-pim)#register mtu 1000
```

```
switch(config-pim)#
```

5.4.27 register probe-interval

Function

The **register probe-interval** command configures the transmission interval of the registration probe packets.

Format

- **register probe-interval** { *probe-interval* | **default** }

Parameters

Parameters	Description	Value
probe-interval	Specifies the transmission interval of the registration probe packets.	It is an integer ranging from 1 to 1799 (unit: s)
default	Uses the default value.	60s

Default Value

60s

View

PIM configuration view

Usage Guidelines

None

Example

Configure the transmission interval of the registration probe packets.

```
switch(config-pim)#register probe-interval 100
switch(config-pim)#
```

5.4.28 register suppression-timeout

Function

The **register suppression-timeout** command configures the time of suppressing registration packets.

Format

- **register suppression-timeout** { *timeout-value* | **default** }

Parameters

Parameters	Description	Value
timeout-value	Specifies the time of suppressing registration packets.	It is an integer ranging from 11 to 3600 (unit: s)
default	Uses the default value.	60s

Default Value

60s

View

PIM configuration view

Usage Guidelines

None

Example

#Configure the time of suppressing registration packets.

```
switch(config-pim)#register suppression-timeout 11
switch(config-pim)#
```

5.4.29 reset pim routing-table

Function

reset pim routing-table command can be used to clear the PIM state of designated downstream interface for the designated PIM table item.

Format

- **reset pim routing-table**

Parameters

None

Default Value

None

View

PIM Configuration View

Usage Guidelines

None

Example

Clear the PIM state of designated downstream interface for the designated PIM table item.

```
switch(config)#ip multicast-routing
switch(config)#pim
switch(config-pim)#reset pim routing-table
switch(config-pim)#
```

5.4.30 rp-address group

Function

rp-address group command can be used to statically configure the RP address of multicast group.
no rp-address group command can be used to delete static RP.

Format

- **rp-address** *ip-address* **group** *prefix-address/prefix-len*
- **rp-address** *ip-address* **group default**
- **no rp-address** *ip-address* **group** *prefix-address/prefix-len*
- **no rp-address** *ip-address* **group default**

Parameters

Parameters	Description	Value
ip-address	RP local address	-
prefix/prefix-len	group address range of RP service	prefix-len is from 0-32

Default Value

None

View

PIM Configuration View

Usage Guidelines

When using this command, group omitted means it is wildcard group.
If only use static RP, then all PIM routers must be configured the same static RP and this is much trouble. So it is recommended to configure staic RP for the BSR router and then transmit to other routers by BSR message. Also user can transmit RP message by configuring candidate RP. If it needs to configure the RP of wildcard group, it needs to designate the wildcard group address. This is different with device of other type.
If the RP has configured multiple multicast group addresses, deleting one existed static RP will result in that all multicast group addresses will be deleted. Currently, it does not afford command for deleting one static RP group address.

Example

Statically configure the RP address of multicast group.

```
switch(config)#ip multicast-routing
switch(config)#pim
switch(config-pim)#rp-address 10.1.1.1 group 224.10.1.1/24
switch(config-pim)#
```

5.4.31 send-check-neighbor {enable|disable}

Function

The **send-check-neighbor {enable|disable}** command enables or disables the PIM neighbor checking. This function ascertains whether to send the Join / Prune and Assert packets to the PIM neighbors. If this function is disabled, the packets will not be sent.

Format

- **send-check-neighbor** { **enable** | **disable** }

Parameters

None

Default Value

None

View

PIM configuration view

Usage Guidelines

None

Example

Enable the PIM neighbor checking.

```
switch(config-pim)#send-check-neighbor enable
switch(config-pim)#
```

5.4.32 source-lifetime

Function

The **source-lifetime** command sets the time-out time of the (S,G) table entry on a switch.

Format

- **source-lifetime** { *time* | **default** }

Parameters

Parameters	Description	Value
time	Specifies the time-out time of the (S,G) table entry on a switch.	It is an integer ranging from 60 to 65535 (unit: s)
default	Uses the default time-out time of the (S,G) table entry on a switch.	The default value is 210s.

Default Value

210s

View

PIM configuration view

Usage Guidelines

None

Example

Set the time-out time of the (S,G) table entry on a switch to 210s.

```
switch(config-pim)#source-lifetime 210
switch(config-pim)#
```

5.4.33 state-refresh-interval

Function

state-refresh-interval command can be used to configure the time interval of sending PIM state refreshing message.

Format

- **state-refresh-interval** { *refresh-interval* | **default** }

Parameters

Parameters	Description	Value
refresh-interval	the time interval of sending PIM state refreshing message	integer, 1-255, unit: second
default	Default Value	60s

Default Value

60s

View

PIM Configuration View

Usage Guidelines

The sending interval of state refreshing message should be less then the keeping joining or prune state timeout.

Example

Configure the time interval of sending PIM state refreshing message to be 50s.

```
switch(config)#ip multicast-routing
switch(config)#pim
switch(config-pim)#state-refresh-interval 50
switch(config-pim)#
```

5.4.34 state-refresh-rate-limit

Function

state-refresh-rate-limit command can be used to configure the minimum time before receiving PIM state refreshing message.

Format

- **state-refresh-rate-limit** { *rate-limit* | **default** }

Parameters

Parameters	Description	Value
rate-limit	the minimum time before receiving PIM state refreshing message	integer, 1-65535, unit: second
default	Default Value	30s

Default Value

30s

View

PIM Configuration View

Usage Guidelines

This command is suitable for the PIM-DM network.
Switch may receive multiple PIM state refreshing messages from multiple Switches in a short time. And some messages are repeated. After using this command, when Switch receiving the first state refreshing message, it will immediately reset related prune timer and start state refreshing timer and the timeout is the waiting time for receiving next state refreshing message.

- The received repeated refreshing message before state refreshing timer is out will be discarded.
- After the state refreshing timer is out, it allows to receive the next state refreshing message.

Example

In the public network instance, configure the minimum time to be 48s before receiving PIM state refreshing message.

```
switch(config)#ip multicast-routing
switch(config)#pim
switch(config-pim)#state-refresh-rate-limit 48
switch(config-pim)#
```

5.4.35 state-refresh-ttl

Function

state-refresh-ttl command can be used to configure the TTL value of sending PIM state refreshing message.

Format

- **state-refresh-ttl** { *refresh-ttl* | **default** }

Parameters

Parameters	Description	Value
refresh-ttl	the TTL value of sending PIM state refreshing message	integer, 1-255, unit: second
default	Default Value	255s

Default Value

255s

View

PIM Configuration View

Usage Guidelines

This command is suitable for the PIM-DM network. After receiving state refreshing message, TTL value will be minus one of Switch. And then it will forward the refreshing message to the downstream until the TTL value is zero. When the network scale is very small, the refreshing message will be circularly transmitted in the network.

Example

Configure the TTL value of sending PIM state refreshing message to be 100s.

```
switch(config)#ip multicast-routing
switch(config)#pim
switch(config-pim)#state-refresh-ttl 100
switch(config-pim)#
```

5.4.36 show ip pim

Function

show ip pim command can be used to display PIM global information.

Format

- **show ip pim**

Parameters

None

Default Value

None

View

Common User View, Privilege User View, Global Configuration View, VLANIF Configuration View

Usage Guidelines

None

Example

#Display PIM global information.

```
switch#show ip pim
  Global information of PIM:
  Ip Multicast Routing                :disable
  Version                              :PIM_VB3.00.00.00
  Instance Max Number                  :127
  Interface Max Number                 :64
  Neighbor Max Number                  :64
  Route Max Number                     :2400
  IP Out Interface Max Number          :4800
  Physical Out Interface Max Number    :4800
  RP Max Number                        :2000
  C-RP Max Number                      :16
  Scope Max Number                     :16
  C-BSR Max Number                     :16
  Border Interface Max Number          :16
switch#
```

5.4.37 show ip pim bsr

Function

show ip pim bsr command can be used to display BSR information.

Format

- **show ip pim bsr**

Parameters

None

Default Value

None

View

Common User View, Privilege User View, Global Configuration View, VLANIF Configuration View

Usage Guidelines

None

Example

#Display BSR information.

```
switch#show ip pim bsr
 Vpn-Instance: N/A
  BSR Address                  :0.0.0.0
  BSR Group                    :224.0.0.0
  BSR Mask Length              :4
  BSR Priority                 :0
  BSR Hash Length              :0
  BSR Expire Time              :0
  CBSR Address                 :--
  CBSR Priority                :0
  CBSR Hash Length             :30
switch#
```

5.4.38 show ip pim c-rp

Function

The **show ip pim c-rp** command displays the information of the candidate RP.

Format

- **show ip pim c-rp**

Parameters

None

Default Value

None

View

Common user view, priviledge user view, global configuration view and VLANIF configuration view

Usage Guidelines

None

Example

View the information of the candidate RP.

```
switch#show ip pim c-rp
 Vpn-Instance: N/A
   C-RP Address                :--
   C-RP Group                  :224.0.0.0
   C-RP Mask Length            :4
   C-RP Priority               :0
   C-RP BSR Address            :0.0.0.0
switch#
```

5.4.39 show ip pim config

Function

show ip pim config command can be used to display configuration information of current operated PIM.

Format

- **show ip pim config**

Parameters

None

Default Value

None

View

Common User View, Privilege User View, Global Configuration View, VLANIF Configuration View

Usage Guidelines

None

Example

#Display configuration information of current operated PIM.

```
switch#show ip pim config
ip multicast-routing
pim
 c-bsr admin-scope enable
 c-bsr send-interval 100
 interface vlan-1
 ip pim-sm
 ip pim c-bsr group default
 ip pim c-rp group default
switch#
```

5.4.40 show ip pim interface

Function

show ip pim interface command can be used to display PIM interface information.

Format

- **show ip pim interface**
- **show ip pim interface vlan** *vlan-id*

Parameters

Parameters	Description	Value
vlan-id	VLAN ID	Integer form with range of 1-4094

Default Value

None

View

Common User View, Privilege User View, Global Configuration View, VLANIF Configuration View

Usage Guidelines

None

Example

#Display PIM interface information.

```
switch#show ip pim interface
  Interface          State      Nbr-Cnt    Hello-Interval  DR-Pri          DR-Address
  vlan-1             down       0          30              1               0.0.0.0
switch#
```

5.4.41 show ip pim neighbor

Function

show ip pim neighbor command can be used to display PIM neighbor information.

Format

- **show ip pim neighbor**
- **show ip pim neighbor** *neighbor-ip-address*

Parameters

Parameters	Description	Value
neighbor-ip-address	Neighbor IP address	Dotted decimal

Default Value

None

View

Common User View, Privilege User View, Global Configuration View, VLANIF Configuration View

Usage Guidelines

None

Example

#Display PIM neighbor information.

```
switch#show ip pim neighbor
  Neighbor-Address   Interface   DRpri          State          ExpiryTime(s)
  10.1.1.1           vlan-1      1              NON-DR         103
switch#
```

5.4.42 show ip pim route

Function

show ip pim route command can be used to display PIM route information.

Format

- **show ip pim route**

- **show ip pim route group** *group-ip-address*
- **show ip pim route group** *group-ip-address* **source** *src-ip-address*
- **show ip pim route group** *group-ip-address* **source** *src-ip-address* **verbose**
- **show ip pim route group** *group-ip-address* **verbose**
- **show ip pim route source** *src-ip-address*
- **show ip pim route source** *src-ip-address* **verbose**
- **show ip pim route verbose**

Parameters

Parameters	Description	Value
src-ip-address	Source IP address	Dotted decimal
group-ip-address	Group IP address	Dotted decimal

Default Value

None

View

Common User View, Privilege User View, Global Configuration View, VLANIF Configuration View

Usage Guidelines

None

Example

#Display PIM route information.

```
switch#show ip pim route
Vpn-Instance: N/A
 (*,225.0.0.1):    RP: 0.0.0.0
 Incoming Interface: N/A, RPF: 0.0.0.0
 Outgoing Interface:
    vlan-1              Forwarding    Expires: 00:00:00
switch#
```

5.4.43 show ip pim rp

Function

show ip pim rp command can be used to display RP information, including local static configured RP information and RP information that was learned from BSR.

Format

- **show ip pim rp**

Parameters

None

Default Value

None

View

Common User View, Privilege User View, Global Configuration View, VLANIF Configuration View

Usage Guidelines

None

Example

Display RP information, including local static configured RP information and RP information that was learned from BSR.

```
switch#show ip pim rp
 Group          RP           Priority     State          BSR-Address              ExpiryTime(s)
Vpn-Instance: N/A
 224.0.0.0/4          10.1.1.3        0          static         0.0.0.0                  0
```

5.4.44 show ip pim rp group

Function

The **show ip pim rp group** command displays the IP address of the elected RP.

Format

- **show ip pim rp group** *group-ip-address*

Parameters

Parameters	Description	Value
group-ip-address	Specifies the group IP address.	The value is in dotted decimal notation.

Default Value

None

View

Common user view, priviledge user view, global configuration view and VLANIF configuration view

Usage Guidelines

This command is used to check the current RP IP address matching the group IP address in real time.

Example

Check the current RP IP address matching the group IP address in real time.

```
switch(config)#show ip pim rp group 225.0.0.1
Elected RP address                : 20.1.1.1
switch(config)#
```

6. Service Security Commands

6.1 Overview

This chapter introduces the service security commands of the N-series switch.

6.2 IP Address Prefix-list Configuration Command

6.2.1 {ip|ipv6} prefix-list

Function

ip prefix-list command can be used to create a filter list that completely matches network segment address with prefix length of MASKLEN (IPv4).
ipv6 prefix-list command can be used to create a filter list that completely matches network segment address with prefix length of MASKLEN (IPv6).

Format

- **ip prefix-list** *list-name* [**index** *index-number*] { **permit | deny** } *ip-address/mask-length*
- **ipv6 prefix-list** *list-name* [**index** *index-number*] { **permit | deny** } *ipv6-address/mask-length*

Parameters

Parameters	Description	Value
list-name	List name that created routing rule belongs to IP type to distinguish different lists	Unique Length range from 1-20 characters
permit	Routing filter rule as permit	-
deny	Routing filter rule as deny	-
index-number	Index number that the filter rule belongs to	Integer form with range of 1-65535
ipv6-address	IPV6 address	-
ip-address	IPV4 address	-
mask-length	Length of address mask	Prefix matching length When it is IPv4 address form the length must not be larger than 32; When it is IPv6 address form, the length must not be larger than 128

Default Value

no list created

View

Global Configuration View

Usage Guidelines

The following issues must be aware when using this command:
The differences of lists are based on Parameters *list-name and* IP address type;
Any rule will be backspaced once matched;
The matching will be performed according to ascending index. If no index is configured, the index number will value as: (largest index number)x 10% + 10.
The latest configuration to index will cover the former configuration.

Example

```
switch(config)#ip prefix-list test permit 1.1.1.1/32
switch(config)#ip prefix-list test index 11 permit 2.2.2.2/32
switch#show ip prefix-list test
ip prefix-list : test
  index: 10       permit 1.1.1.1/32
  index: 11       permit 2.2.2.2/32

switch(config)#ipv6 prefix-list test permit 1::1/32
switch(config)#ipv6 prefix-list test index 12 permit 2::2/32
switch(config)#show ipv6 prefix-list test
ipv6 prefix-list : test
  index: 10       permit 1::1/32
  index: 12       permit 2::2/32
```

6.2.2 {ip|ipv6} prefix-list greater-equal

Function

ip prefix-list greater-equal command can be used to create a filter rule that the mask length of route address is no smaller than designated minimum value and completely matches network segment address with prefix mask length (IPv4).
ipv6 prefix-list greater-equal command can be used to create a filter rule that the mask length of route address is no smaller than designated minimum value and completely matches network segment address with prefix mask length (IPv6).

Format

- **ip prefix-list** *list-name* [**index** *index-number*] { **deny** | **permit** } *ip-address/mask-length* **greater-equal** *min-range*
- **ipv6 prefix-list** *list-name* [**index** *index-number*] { **deny** | **permit** } *ipv6-address/mask-length* **greater-equal** *min-range*

Parameters

Parameters	Description	Value
list-name	List name that created routing rule belongs to IP type to distinguish	Unique Length range: 1-20 characters

Parameters	Description	Value
	different lists	
permit	Routing filter rule as permit	-
deny	Routing filter rule as deny	-
index-number	Index number that the filter rule belongs to	Integer form with range of 1-65535
ipv6-address	IPV6 address	-
ip-address	IPV4 address	-
mask-length	Length of address mask	Prefix matching length When it is IPv4 address form the length must not be larger than 32; When it is IPv6 address form, the length must not be larger than 128
min-range	Minimum length of mask address	IPv4:0~32; IPv6: 0~128

Default Value

no list created

View

Global Configuration View

Usage Guidelines

The following issues must be aware when using this command:

- The differences of lists are based on Parameters *list-name and* IP address type;
- Any rule will be backspaced once matched;
- The matching will be performed according to ascending index. If no index is configured, the index number will value as: (largest index number)x 10% + 10.
- No check to list index relationship and logic antinomy, please arrange on-demand when configuring;
- The latest configuration to index will cover the former configuration.

Example

```
switch(config)#ip prefix-list test permit 1.1.1.1/32 greater-equal 32
switch(config)#ip prefix-list test index 11 permit 2.2.2.2/32 greater-equal 32
switch(config)#show ip prefix-list test
ip prefix-list : test
  index: 10       permit 1.1.1.1/32                    10ge1/0/19       le 32
  index: 11       permit 2.2.2.2/32                    10ge 1/0/19      le 32

switch(config)#ipv6 prefix-list test permit 1::1/32 greater-equal 38
```

```
switch(config)#ipv6 prefix-list test index 14 permit 2::2/32 greater-equal 38
switch(config)#show ipv6 prefix-list test
ipv6 prefix-list : test
 index: 10      permit 1::1/32                  10ge1/0/ 38      le 128
 index: 14      permit 2::2/32                  10ge1/0/38       le 128
```

6.2.3 {ip|ipv6} prefix-list less-equal

Function

ip prefix-list less-equal command can be used to create a filter rule that the mask length of routing address is no larger than designated maximum value and completely matches network segment address of prefix mask length (IPv4).
ipv6 prefix-list less-equal command can be used to create a filter rule that the mask length of routing address is no larger than designated maximum value and completely matches network segment address of prefix mask length (IPv6).

Format

- **ip prefix-list** *list-name* [**index** *index-number*] { **deny** | **permit** } *ip-address/mask-length* **less-equal** *max-range*
- **ipv6 prefix-list** *list-name* [**index** *index-number*] { **deny** | **permit** } *ipv6-address/mask-length* **less-equal** *max-range*

Parameters

Parameters	Description	Value
list-name	List name that created routing rule belongs to IP type to distinguish different lists	Unique Length range: 1-20characters
permit	Routing filter rule as permit	-
deny	Routing filter rule as deny	-
index-number	Index number that the filter rule belongs to	Integer form with range of 1-65535
ipv6-address	IPV6 address	-
ip-address	IPV4 address	-
mask-length	Length of address mask	Prefix matching length When it is IPv4 address form the length must not be larger than 32; When it is IPv6 address form, the length must not be larger than 128
max-range	Maximum length of mask address	IPv4:0~32; IPv6: 0~128

Default Value

no list created

View

Global Configuration View

Usage Guidelines

The following issues must be aware when using this command:

- The differences of lists are based on Parameters *list-name and* IP address type;
- Any rule will be backspaced once matched;
- The matching will be performed according to ascending index. If no index is configured, the index number will value as: (largest index number)x 10% + 10.
- No check to list index relationship and logic antinomy, please arrange on-demand when configuring;
- The latest configuration to index will cover the former configuration.

Example

```
switch(config)#ip prefix-list test permit 1.1.1.1/32 less-equal 32
switch(config)#ip prefix-list test index 44 permit 2.2.2.2/32 less-equal 32
switch(config)#show ip prefix-list test
ip prefix-list : test
  index: 10      permit 1.1.1.1/32                  10ge1/0/ 16      le 32
  index: 44      permit 2.2.2.2/32                  10ge1/0/ 16      le 32

switch(config)#ipv6 prefix-list test permit 1::1/32 less-equal 38
switch(config)#ipv6 prefix-list test index 11 permit 2::2/32 less-equal 38
switch(config)#show ipv6 prefix-list test
ipv6 prefix-list : test
  index: 10      permit 1::1/32                     10ge1/0/ 32      le 38
  index: 11      permit 2::2/32                     10ge1/0/ 32      le 38
```

6.2.4 {ip|ipv6} prefix-list greater-equal less-equal

Function

ip prefix-list greater-equal less-equal command can be used to create a filter rule that mask length of routing address is no larger than the one between designated minimum and maximum value, and completely matches network segment address of prefix mask length (IPv4).

ipv6 prefix-list greater-equal less-equal command can be used to create a filter rule that mask length of routing address is no larger than the one between designated minimum and maximum value, and completely matches network segment address of prefix mask length (IPv6).

Format

- **ip prefix-list** *list-name* [**index** *index-number*] { **deny** | **permit** } *ip-address/mask-length* **greater-equal** *min-range* **less-equal** *max-range*
- **ipv6 prefix-list** *list-name* [**index** *index-number*] { **deny** | **permit** } *ipv6-address/mask-length* **greater-equal** *min-range* **less-equal** *max-range*

Parameters

Parameters	Description	Value
list-name	List name that created routing rule belongs to IP type to distinguish different lists	Unique Length range: 1-20 characters
permit	Routing filter rule as permit	-
deny	Routing filter rule as deny	-
index-number	Index number that the filter rule belongs to	Integer form with range of 1-65535
ipv6-address	IPV6 address	-
ip-address	IPV4 address	-
mask-length	Length of address mask	Prefix matching length When it is IPv4 address form the length must not be larger than 32; When it is IPv6 address form, the length must not be larger than 128
min-range	Minimum length of mask address	IPv4:0~32; IPv6: 0~128
max-range	Maximum length of mask address	IPv4:0~32; IPv6: 0~128

Default Value

no list created

View

Global Configuration View

Usage Guidelines

The following issues must be aware when using this command:

- The differences of lists are based on Parameters *list-name and* IP address type;
- Any rule will be backspaced once matched;
- The matching will be performed according to ascending index. If no index is configured, the index number will value as: (largest index number)x 10% + 10.
- No check to list index relationship and logic antinomy, please arrange on-demand when configuring;
- The latest configuration to index will cover the former configuration.

Example

```
switch(config)#ip prefix-list test permit 1.1.1.1/32 greater-equal 32 less-equal 32
switch(config)#ip prefix-list test index 280 permit 2.2.2.2/32 greater-equal 32 less-equal 32
switch(config)#show ip prefix-list test
```

```
ip prefix-list : test
 index: 10       permit 1.1.1.1/32                10ge1/0/ 32       le 32
 index: 280      permit 2.2.2.2/32                10ge1/0/ 32       le 32

switch(config)#ipv6 prefix-list test permit 1::1/32 greater-equal 35 less-equal 38
switch(config)#ipv6 prefix-list test index 22 permit 2::2/32 greater-equal 37 less-equal 38
switch(config)#show ipv6 prefix-list test
ipv6 prefix-list : test
 index: 10       permit 1::1/32                   10ge1/0/ 35       le 38
 index: 22       permit 2::2/32                   10ge1/0/ 37       le 38
```

6.2.5 no {ip|ipv6} prefix-list

Function

no ip prefix-list command can be used to delete rule from the filter rule list (IPv4).
no ipv6 prefix-list command can be used to delete rule from the filter rule list (IPv6).

Format

- **no ip prefix-list** *list-name* [**index** *index-number*]
- **no ipv6 prefix-list** *list-name* [**index** *index-number*]

Parameters

Parameters	Description	Value
list-name	List name that created routing rule belongs to IP type to distinguish different lists	Unique Length range: 1-20 characters
index-number	Index number that the filter rule belongs to	Integer form with range of 1-65535

Default Value

None

View

Global Configuration View

Usage Guidelines

None

Example

- switch(config)#no ip prefix-list test
- switch(config)#

6.2.6 show {ip|ipv6} prefix-list

Function

show ip prefix-list command can be used to display rules in the filter rule list (IPv4).
show ipv6 prefix-list command can be used to display rules in the filter rule list (IPv6).

Format

- **show ip prefix-list** [*list-name*]
- **show ipv6 prefix-list** [*list-name*]

Parameters

Parameters	Description	Value
list-name	List name that created routing rule belongs to IP type to distinguish different lists	Unique Length range: 1-20 characters

Default Value

None

View

Common User View, Privilege User View, Global Configuration View

Usage Guidelines

If the rule name is not designated when using this command, it indicates to display the content to the rules with all same address type

Example

```
switch#show ip prefix-list
ip prefix-list : test
  index: 10       permit 1.1.0.0/16
  index: 11       permit 2.2.0.0/16
ip prefix-list : tes
  index: 11       permit 2.2.0.0/16
switch#
```

6.2.7 show ip prefix-list information

Function

The **show ip prefix-list information** command displays the rules of the IP address prefix (for IPv4).

Format

- **show ip prefix-list information**

Parameters

None

Default Value

None

View

Common user view, priviledge user view and global configuration view

Usage Guidelines

None

Example

View the rules of the IP address prefix.

```
switch#show ip prefix-list information
 Version IPPREFIX_VB3.00.10.00
 ipprefix global structure size 192
 RouteSocket=3
 Memory Statistics
 Configuration Params:
 List:32
 Rule:256

 Total Allocate memory:28672 Bytes

 Detailed Memory Operation
 Index      Add        Fail       Free       Current    Size       Description
 0          0          0          0          0          224        Ip Prefix List
 1          0          0          0          0          84         Ip Prefix Rule
switch#
```

6.2.8 ACL Configuration Commands

6.2.9 filter-list

Function

The **filter-list** command creates a numbered access control list (ACL) and displays the ACL view.
The **no filter-list** command deletes the ACL with a specified number.

Format

- **filter-list** *acl-number* [**name** *filter-name*]**no filter-list** *acl-number*

Parameters

Parameters	Description	Value
acl-number	Specifies the ACL number.	The value is an integer ranging from 1 to 4000. <1-1000> specify an L2 ACL. <1001-2000> specify an IPv4 ACL. <2001-3000> specify a hybrid ACL. <3001-4000> specify an IPv6 ACL.
filter-name	Specifies the ACL name.	The value is a character string.

Default Value

None

View

Global configuration view

Usage Guidelines

One ACL consists of several ACL rules.
When creating an ACL, you need to specify a number, indicating the ACL category. For example, a number ranging from 1 to 1000 indicates a basic layer 2 ACL.

Note: An ACL must be created before defining ACL rules.

Warning: Before configuring ACL functions, you must bind the ACL with filter entries.

```
switch(config)#filter-list 100
switch(configure-filter-l2-100)#
switch(configure-filter-l2-100)#filter 100 mac any any
switch(configure-filter-l2-100)#
…
switch(config)#interface 10gigaethernet 1/0/1
switch(config-10ge1/0/1)#filter-list in 100
switch(config)#
```

Example

Create an ACL numbered 100.

```
switch(config)#filter-list 100
switch(configure-filter-l2-100)#

switch(config)#no filter-list 100
switch(config)#
```

6.2.10 filter-list {in|out}

Function

The **filter-list {in|out}** command applies an ACL to a physical port, a trunk interface, or a VLAN port.
The **no filter-list {in|out}** command cancels the application of an ACL to a physical port, a trunk interface, or a VLAN port.

Format

- **filter-list** { **in** | **out** } *acl-number*
- **filter-list** { **in** | **out** } **name** *filter-name*
- **no filter-list** { **in** | **out** } [*acl-number*]

Parameters

Parameters	Description	Value
acl-number	Specifies the ACL number.	The value is an integer in the range from 1 to 4000.
filter-name	Specifies the ACL name.	The value is a character string.

Default Value

None

View

Interface configuration view (Ethernet and trunk), VLANIF configuration view, interface group configuration view

Usage Guidelines

You can use this command to apply an ACL to a physical port or a trunk interface in the port configuration view. The function of this command is the same as that of the filter-list global command in the global configuration view. You can select the commands according to actual requirements.

Example

Enter the configuration view of a port and bind it with the ACL 100.

```
switch(config)#interface 100gigaethernet 1/0/1
switch(config-100ge1/0/1)#filter-list in 100
switch(config-100ge1/0/1)#
```

Enter the configuration view of a Trunk and bind it with the ACL 100.

```
switch(config)#interface eth-trunk 2
switch(config-eth-trunk-2)#filter-list in 100
switch(config-eth-trunk-2)#
```

6.2.11filter action {permit|deny}

Function

The **filter action {permit|deny}** command sets the action for an ACL rule to permit or deny, which means to forward or drop packets matching the rule.

Format

- **filter** *rule-number* **action** { **permit** | **deny** }

Parameters

Parameters	Description	Value
rule-number	Specifies the ACL number.	The value is an integer in the range from 1 to 2048.
permit	Permits packets in compliance with ACL rules.	-
deny	Denies packets in compliance with ACL rules.	-

Default Value

None

View

Filter configuration view

Usage Guidelines

If the action defined in the ACL rule is **deny**, a packet matching the ACL rule will be dropped.
If the action defined in the ACL rule is **permit**, a packet matching the ACL rule will be forwarded or processed.

Example

Set the action in rule 1 of ACL 100 to deny.

```
switch(configure-filter-l2-100)#filter 100 action deny
switch(configure-filter-l2-100)#
```

6.2.12 filter ip

Function

The **filter ip** command configures an ACL rule matching packets based on source and destination IPv4 addresses.

Format

- **filter** *rule-number* **ip** { *src-ip-address/M* | **any**} { *dst-ip-address/M* | **any** }

Parameters

Parameters	Description	Value
rule-number	Specifies the ACL number.	The value is an integer in the range from 1 to 2048.
src-ip-address/M | **any**	Specifies the source IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. **any** means any source IP address.
dst-ip-address/M | **any**	Specifies the destination IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. **any** means any destination IP address.

Default Value

None

View

Filter configuration view (IPv4 and hybrid)

Usage Guidelines

After the ACL entry is applied, a port filters received packets according to the IP addresses in the packets. The port takes the corresponding actions for packets matching the ACL rule.

Warning: The ACL list is classified to four levels. The filter ip is applicable only to IPv4 / hybrid ACLs 1001 to 4000.

```
switch(config)#filter-list
  <1-1000>       L2 filter list number
  <1001-2000>    IPv4 filter list number
  <2001-3000>    Hybrid filter list number
  <3001-4000>    IPv6 filter list number
```

Example

Configure an ACL rule based on the source and destination IPv4 address.

```
switch(configure-filter-ipv4-2000)#filter 100 ip 1.1.1.1/10 2.2.2.2/20
switch(configure-filter-ipv4-2000)#
```

6.2.13 filter ip dscp

Function

The **filter ip dscp** command configures an ACL rule matching packets based on source and destination IPv4 addresses and the DSCP field.

Format

- **filter** *rule-number* **ip** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } **dscp** *dscp*

Parameters

Parameters	Description	Value
rule-number	Specifies the ACL number.	The value is an integer in the range from 1 to 2048.
src-ip-address/M | **any**	Specifies the source IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any source IP address.
dst-ip-address/M | **any**	Specifies the destination IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any destination IP address.
dscp	Distinguishes the values of service code points.	The DSCP value is an integer or a name. When the value is an integer, it ranges from 0 to 63. When the value is a name, it is af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, or ef.

default Value

None

View

Filter configuration view (IPv4 and hybrid)

Usage Guidelines

After the ACL entry is applied, a port filters received packets according to the IP addresses and DSCP field in the packets. The port takes the corresponding actions for packets matching the ACL rule.

Example

Configure an ACL rule matching packets based on source and destination IPv4 addresses and the DSCP field.

```
switch(configure-filter-ipv4-1500)#filter 100 ip 1.1.1.1/10 2.2.2.2/20 dscp 10
switch(configure-filter-ipv4-1500)#
```

6.2.14 filter ip fragment

Function

The **filter ip fragment** command configures an ACL rule matching packets based on source and destination IPv4 addresses and the fragment field.

Format

- **filter** *rule-number* **ip** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } **fragment**

Parameters

Parameters	Description	Value
rule-number	Specifies the ACL number.	The value is an integer in the range from 1 to 2048.
src-ip-address/M| **any**	Specifies the source IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any source IP address.
dst-ip-address/M | **any**	Specifies the destination IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any destination IP address.
fragment	Specifies whether the rule is valid for the non-first fragment message only.	-

Default Value

None

View

Filter configuration view (IPv4 and hybrid)

Usage Guidelines

After the ACL entry is applied, the switch matches the IP addresses in the received packets and determines whether the packets are non-first fragment packets. If the IP addresses of the packets match the ACL rule and the packets are non-first fragment packets, the switch takes the corresponding actions for packets according to the ACL rule.

Example

Configure an ACL rule matching packets based on source and destination IPv4 addresses and the fragment field.

```
switch(configure-filter-ipv4-1500)#filter 100 ip 1.1.1.1/10 2.2.2.2/20 fragment
switch(configure-filter-ipv4-1500)#
```

6.2.15 filter ip precedence

Function

The **filter ip precedence** command configures an ACL rule matching packets based on source and destination IPv4 addresses and the TOS field.

Format

- **filter** *rule-number* **ip** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } **precedence** *tos-priority*

Parameters

Parameters	Description	Value
rule-number	Specifies the ACL number.	The value is an integer in the range from 1 to 2048.
src-ip-address/M | **any**	Specifies the source IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any source IP address.
dst-ip-address/M | **any**	Specifies the destination IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. **any** means any destination IP address.
tos-priority	Specifies the priority of the TOS field.	The value is an integer in the range from 0 to 7.

Default Value

None

View

Filter configuration view (IPv4 and hybrid)

Usage Guidelines

After the ACL entry is applied, a port filters received packets according to the IP addresses and TOS field in the packets. The port takes the corresponding actions for packets matching the ACL rule.

Example

Configure an ACL rule matching packets based on source and destination IPv4 addresses and the TOS field.

```
switch(configure-filter-ipv4-1500)#filter 100 ip 1.1.1.1/10 2.2.2.2/20 precedence 1
switch(configure-filter-ipv4-1500)#
```

6.2.16 filter ip precedence fragment

Function

The **filter ip precedence fragment** command configures an ACL rule matching packets based on source and destination IPv4 addresses, TOS field, and the fragment field.

Format

- **filter** *rule-number* **ip** { *src-ip-address/M* | **any**} { *dst-ip-address/M* | **any** } **precedence** *tos-priority* **fragment**

Parameters

Parameters	Description	Value
rule-number	Specifies a filter number.	The value is an integer in the range from 1 to 2048.
src-ip-address/M| **any**	Specifies the source IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any source IP address.
dst-ip-address/M | **any**	Specifies the destination IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any destination IP address.
tos-priority	Specifies the TOS field in an ACL rule.	The value is an integer in the range from 0 to 7.
fragment	Specifies whether the rule is valid for the non-first fragment message only.	-

Default Value

None

View

Filter configuration view (IPv4 and hybrid)

Usage Guidelines

None

Example

Configure an ACL rule matching packets based on source and destination IPv4 addresses, the ToS field, and the fragment field.

```
switch(configure-filter-ipv4-1500)#filter 100 ip 1.1.1.1/10 2.2.2.2/20 precedence 1 fragment
switch(configure-filter-ipv4-1500)#
```

6.2.17 filter ip proto-type

Function

The **filter ip proto-type** command configures an ACL rule based on the source/destination IPv4 address and protocol type field.

Format

- **filter** *rule-number* **ip** { *src-ip-address/M* | **any** } { *dst-ip-address M* | **any** } **proto-type** *proto-type-value*

Parameters

Parameters	Description	Value
rule-number	Specifies a filter number.	The value is an integer in the range from 1 to 2048.
src-ip-address/M| **any**	Specifies the source IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any source IP address.
dst-ip-address/M | **any**	Specifies the destination IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any destination IP address.
proto-type-value	Specifies the protocol type in an ACL rule.	The value is an integer in the range from 1 to 255.

Default Value

None

View

Filter configuration view (IPv4 and hybrid)

Usage Guidelines

None

Example

Configure an ACL rule matching packets based on the source and destination IPv4 addresses and the protocol type field.

```
switch(configure-filter-ipv4-1500)#filter 100 ip 1.1.1.1/10 2.2.2.2/20 proto-type 10
switch(configure-filter-ipv4-1500)#
```

6.2.18 filter ip tos

Function

The **filter ip tos** command configures an ACL rule based on the source/destination IPv4 address and ToS field.

Format

- **filter** *rule-number* **ip** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } **tos** *tos-value*
- **filter** *rule-number* **ip** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } **tos** *tos-value* **fragment**

Parameters

Parameters	Description	Value
rule-number	Specifies a filter number.	The value is an integer in the range from 1 to 2048.
src-ip-address/M| **any**	Specifies the source IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any source IP address.
dst-ip-address/M | **any**	Specifies the destination IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any destination IP address.
tos-value	Specifies the TOS in an ACL rule.	The value is an integer in the range from 0 to 15.

Default Value

None

View

Filter configuration view (IPv4 and hybrid)

Usage Guidelines

None

Example

Configure an ACL rule matching packets based on the source and destination IPv4 addresses and the ToS field.

```
switch(configure-filter-ipv4-1500)#filter 100 ip 1.1.1.1/10 2.2.2.2/20 tos 10
switch(configure-filter-ipv4-1500)#
```

6.2.19 filter ip ttl

Function

The **filter ip ttl** command configures an ACL rule based on the source/destination IPv4 address and TTL field.

Format

- **filter** *rule-number* **ip** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } **ttl** *ttl-value*

Parameters

Parameters	Description	Value
rule-number	Specifies a filter number.	The value is an integer in the range from 1 to 2048.

Parameters	Description	Value
src-ip-address/M| **any**	Specifies the source IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any source IP address.
dst-ip-address/M | **any**	Specifies the destination IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any destination IP address.
ttl-value	Specifies the TTL in an ACL rule.	The value is an integer in the range from 1 to 255.

Default Value

None

View

Filter configuration view (IPv4 and hybrid)

Usage Guidelines

None

Example

Configure an ACL rule based on the source/destination IPv4 address and TTL field.

```
switch(configure-filter-ipv4-1500)#filter 100 ip 1.1.1.1/10 2.2.2.2/20 ttl 20
switch(configure-filter-ipv4-1500)#
```

6.2.20 filter icmp

Function

The **filter icmp** command configures an ACL rule matching packets based on source and destination IPv4 addresses and the ICMP field.

Format

- **filter** *rule-number* **icmp** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** }
- **filter** *rule-number* **icmp** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } { *icmp-type* | **any** } { *icmp-code* | **any** }

Parameters

Parameters	Description	Value
rule-number	Specifies a filter number.	The value is an integer in the range from 1 to 2048.

Parameters	Description	Value
src-ip-address/M| **any**	Specifies the source IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any source IP address.
dst-ip-address/M | **any**	Specifies the destination IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. **any** means any destination IP address.
icmp-type	Specifies the ICMP type range in an ACL rule.	The value is an integer in the range from 0 to 255.
icmp-code	Specifies the ICMP code range in an ACL rule.	The value is an integer in the range from 0 to 255.

Default Value

None

View

Filter configuration view (IPv4 and hybrid)

Usage Guidelines

None

Example

Configure an ACL rule matching packets based on source and destination IPv4 addresses and the ICMP field.

```
switch(configure-filter-ipv4-1500)#filter 100 icmp 1.1.1.1/10 2.2.2.2/20 20 30
switch(configure-filter-ipv4-1500)#
```

6.2.21 filter igmp

Function

The **filter igmp** command configures an ACL rule based on the source/destination IPv4 address and IGMP type ID field.

Format

- **filter** *rule-number* **igmp** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** }

Parameters

Parameters	Description	Value
rule-number	Specifies a filter number.	The value is an integer in the range from 1 to 2048.
src-ip-address/M| **any**	Specifies the source IP address	The value of *src-ip-address* is in the

Parameters	Description	Value
	in an ACL rule.	dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any source IP address.
dst-ip-address/M | **any**	Specifies the destination IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any destination IP address.

Default Value

None

View

Filter configuration view (IPv4 and hybrid)

Usage Guidelines

None

Example

Configure an ACL rule matching packets based on source and destination IPv4 addresses and the IGMP type ID field.

```
switch(configure-filter-ipv4-1500)#filter 100 igmp 1.1.1.1/10 2.2.2.2/20
switch(configure-filter-ipv4-1500)#
```

6.2.22 filter tcp

Function

The **filter tcp** command configures an ACL rule matching packets based on source and destination IPv4 addresses and the TCP fields (including syn, synack, ack, and fin fields).

Format

- **filter** *rule-number* **tcp** { *src-ip-address/M* | **any** } { *src-port-number* | **any** | *source-port-number-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *destination-port-number-range* }
- **filter** *rule-number* **tcp** { *src-ip-address/M* | **any** } { *src-port-number* | **any** | *source-port-number-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *destination-port-number-range* } { **syn** | **synack** | **ack** | **fin** }
- **filter** *rule-number* **tcp** { *src-ip-address/M* | **any** } { *src-port-number* | **any** | *source-port-number-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *destination-port-number-range* } { **syn** | **synack** | **ack** | **fin** } **fragment**
- **filter** *rule-number* **tcp** { *src-ip-address/M* | **any** } { *src-port-number* | **any** | *source-port-number-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *destination-port-number-range* } **fragment**

Parameters

Parameters	Description	Value
rule-number	Specifies a filter number.	The value is an integer in the range from 1 to 2048.
src-ip-address/M| **any**	Specifies the source IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any source IP address.
dst-ip-address/M | **any**	Specifies the destination IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any destination IP address.
src-port-number	Specifies the source port number.	The value is an integer in the range of <0-65535>.
dst-port-number	Specifies the destination port number.	The value is an integer in the range of <0-65535>.
source-port-number-range destination-port-number-range	Specifies the source port number range and destination port number range.	The value is an integer ranging from 0-65535 / 0-65535.
fragment	Specifies whether the rule is valid for the non-first fragment message only.	-

Default Value

None

View

Filter configuration view (IPv4 and hybrid)

Usage Guidelines

None

Example

Configure an ACL rule matching packets based on source and destination IPv4 addresses and the TCP fields (including syn, synack, ack, and fin fields).

```
switch(configure-filter-ipv4-1500)#filter 100 tcp 1.1.1.1/10 any 2.2.2.2/20 any syn fragment
switch(configure-filter-ipv4-1500)#
```

6.2.23 filter udp

Function

The **filter udp** command configures an ACL rule matching packets based on source and destination IPv4 addresses and the UDP field.

Format

- **filter** *rule-number* **udp** { *src-ip-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* }
- **filter** *rule-number* **udp** { *src-ip-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* } **fragment**

Parameters

Parameters	Description	Value
rule-number	Specifies a filter number.	The value is an integer in the range from 1 to 2048.
src-ip-address/M| **any**	Specifies the source IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any source IP address.
dst-ip-address/M | **any**	Specifies the destination IP address in an ACL rule.	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 32. The field **any** means any destination IP address.
src-port-number	Specifies the source port number.	The value is an integer in the range from 0 to 65535.
src-port-range	Specifies the source port number range.	The value is an integer ranging from 0-65535 / 0-65535.
dst-port-number	Specifies the destination port number.	The value is an integer in the range from 0 to 65535.
dst-port-range	Specifies the destination port number range.	The value is an integer ranging from 0-65535 / 0-65535.
fragment	Specifies whether the rule is valid for the non-first fragment message only.	-

Default Value

None

View

Filter configuration view (IPv4 and hybrid)

Usage Guidelines

None

Example

Configure an ACL rule matching packets based on source and destination IPv4 addresses and the UDP field.

```
switch(configure-filter-ipv4-1500)#filter 100 udp 1.1.1.1/10 any 2.2.2.2/20 any fragment
switch(configure-filter-ipv4-1500)#
```

6.2.24 filter mac

Function

The **filter mac** command configures an ACL rule matching packets based on MAC address entries.

Format

Filter configuration view (L2 and hybrid)

- **filter** *rule-number* **mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** }
- **filter** *rule-number* **mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** } { **customer** | **provider** } { **any** | *vlan-id* | *vlan-id1/vlan-id2* } { **any** | *priority* }
- **filter** *rule-number* **mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** } **eth-type** { **ip** | **arp** | *digital-protocol-value* }
- **filter** *rule-number* **mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** } **provider** *vlan-id1/vlan-id2* { **any** | *priority* } **customer** { **any** | *vlan-id* } { **any** | *priority* }
- **filter** *rule-number* **mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** } **provider** { **any** | *vlan-id* } { **any** | *priority* } **customer** *vlan-id1/vlan-id2* { **any** | *priority* }
- **filter** *rule-number* **mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** } **provider** { **any** | *vlan-id* } { **any** | *priority* } **customer** { **any** | *vlan-id* } { **any** | *priority* }

Filter configuration view (hybrid)

- **filter** *rule-number* **mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** } **eth-type** { **ip** | **arp** | *digital-protocol-value* }

Parameters

Parameters	Description	Value
rule-number	Specifies a filter number.	The value is an integer in the range from 1 to 2048.
src-mac-address/M| **any**	Specifies the source MAC address in an ACL rule.	*M* is an integer in the range from 1 to 48. **any** means any source MAC address.
dst-mac-address/M |**any**	Specifies the destination MAC address in an ACL rule.	*M* is an integer in the range from 1 to 48. **any** means any destination MAC address.
vlan-id，vlan-id1/vlan-id2	Specifies the VID or VID range.	The value is an integer in the range from 1 to 4094.
priority	Specifies the Dot1p priority.	The value is an integer in the range from 0 to 7.
digital-protocol-value	Specified the protocol value.	The value is an integer ranging from 0x0600 to 0xfffe.
src-ip-address/M	Specifies the length of the source IP address and mask.	The value is in dotted decimal notation.
dst-ip-address/M	Specifies the length of the	The value is in dotted decimal notation.

Parameters	Description	Value
	destination IP address and mask.	
protocol-type-value	Specified the protocol type value.	The value is an integer in the range from 1 to 255.

Default Value

None

View

Filter configuration view (L2 and hybrid)

Usage Guidelines

None

Example

Configure an ACL rule matching packets based on MAC addresses.

```
switch(configure-filter-l2-100)#filter 100 mac 11:11:11:11:11:11/10 22:22:22:22:22:22/20 customer 10 1
switch(configure-filter-l2-100)#
```

6.2.25 no filter

Function

The **no filter** command deletes an ACL rule.

Format

- **no filter** *rule-number*

Parameters

Parameters	Description	Value
rule-number	Specifies a filter number.	The value is an integer in the range from 1 to 2048.

Default Value

None

View

Filter configuration view

Usage Guidelines

None

Example

Delete an ACL rule.

```
switch(configure-filter-ipv4-1500)#no filter 100
switch(configure-filter-ipv4-1500)#
```

6.2.26 show filter-list

Function

The **show filter-list** command displays the ACL configuration.

Format

- **show filter-list**
- **show filter-list** *acl-number*

Parameters

Parameters	Description	Value
acl-number	(Optional) Specifies the number of the ACL to be checked.	The value is an integer in the range from 1 to 4000.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), VLANIF configuration view, VLAN configuration view, Filter configuration view, and interface group configuration view

Usage Guidelines

If *acl-number* is not configured, all ACL categories and all ACL rules under each ACL category will be displayed. If *acl-number* is specified, the command displays information about the specified ACL.

Example

Show the configuration of the ACL.

```
switch#show filter-list
 filter-list 1 name acl1 filter 0
filter-list 1 name acl1
switch#
```

6.2.27 show filter-list brief

Function

The **show filter-list brief** command shows brief ACL information.

Format

- **show filter-list brief**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), VLANIF configuration view, VLAN configuration view, Filter configuration view, and interface group configuration view

Usage Guidelines

None

Example

Show brief ACL information.

```
switch(config)#show filter-list brief
Filter-List       RuleNumber    Name
 1                    0                acl1
switch(config)#
```

6.2.28 show filter-list config

Function

The **show filter-list config** command displays the ACL configuration file information on the switch.

Format

- **show filter-list config**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), VLANIF configuration view, VLAN configuration view, Filter configuration view, and interface group configuration view

Usage Guidelines

None

Example

Show ACL configuration file information.

```
switch(config)#show filter-list config
filter-list 1 name acl1 filter 0
filter-list 1 name acl1


switch(config)#
```

6.2.29 show filter-list interface

Function

The **show filter-list interface** command displays information about all interfaces with ACLs applied.

Format

- **show filter-list interface**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), VLANIF configuration view, VLAN configuration view, Filter configuration view, and interface group configuration view

Usage Guidelines

You can use this command to check the information of ACL-enabled ports.

Example

Display information about all interfaces with ACLs applied.

```
switch(config-10ge1/0/1)#show filter-list interface
Filter-list Interface          Dir Name
   1        10ge-1/0/1            In   acl1
switch(config-10ge1/0/1)#
```

6.2.30 show filter-list name

Function

The **show filter-list name** command shows the configuration of the ACL.

Format

- **show filter-list name** *acl-name*

Parameters

Parameters	Description	Value
acl-name	Specifies the name of a to-be-viewed ACL.	The value is a character string.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), VLANIF configuration view, VLAN configuration view, Filter configuration view, and interface group configuration view

Usage Guidelines

None

Example

Show the configuration of the ACL.

```
switch#show filter-list name acl1
filter-list 1 name acl1 filter 1
filter-list 1 name acl1
 filter 1 mac any 00:00:00:00:00:01/48
 filter 1 action deny

switch#
```

6.2.31 show filter-list statistic

Function

The **show filter-list statistic** command shows the statistics of the ACL.

Format

- **show filter-list statistic**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), VLANIF configuration view, VLAN configuration view, Filter configuration view, and interface group configuration view

Usage Guidelines

The statistics of the ACL includes the Direction, Packets, Bytes, Interface, and SwCounterId.

Example

Show the statistics of an ACL.

```
switch#show filter-list statistic
  Dir=Direction
  P=Packets
  B=Bytes
  Index Interface Dir SwCounterId Green(P|B) Red(P|B) Yellow(P|B) Total(P|B)
switch#
```

6.2.32 counter

Function

The **counter** command is used together with the ACL. You can use this command to bind a filter entry in an ACL.

Format

- **counter** *counter-number* **packet sort** { **green** | **red** | **greenred** | **greenyellow** | **redyellow** | **total** }
- **no counter** *counter-number*

Parameters

Parameters	Description	Value
counter-number	Specifies the counter number.	The value is an integer in the range from 1 to 1024.
packet	Specifies the packet type.	-
green/red/greenred/greenyellow/redyellow|total	Specifies the counter state display type, including green, red, green/red, green/yellow, and red/yellow.	-

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Bind a filter entry in an ACL.

```
switch(config)#counter 100 packet sort green
switch(config)#
```

6.2.33 show counter

Function

The **show counter** command shows counter information and configuration.

Format

- **show counter**
- **show counter** *counter-number*
- **show counter config**

Parameters

Parameters	Description	Value
counter-number	Specifies the counter ID.	The value is an integer in the range from 1 to 1024.

Default Value

None

View

Privileged user view and global configuration view

Usage Guidelines

None

Example

Show counter information.

```
switch(config)#show counter
```

```
Version is COUNTER_VB3.00.00.00
   The total number of counter is :0
switch(config)#
```

6.3 IPv6 ACL Configuration Commands

6.3.1 filter icmp6

Function

The **filter icmp6** command configures an ACL rule based on the source/destination IPv6 address and ICMP6 field.

Format

- **filter** *rule-number* **icmp6** { *src-ip6-address/M* | **any**} { *dst-ip6-address/M* | **any** }
- **filter** *rule-number* **icmp6** { *src-ip6-address/M* | **any**} { *dst-ip6-address/M* | **any** } { *icmp-type* | **any** } { *icmp-code* | **any** }

Parameters

Parameters	Description	Value
rule-number	Specifies a filter number.	The value is an integer in the range from 1 to 2048.
src-ip6-address/M| **any**	Specifies the source IP address of the designated ACL rule	The value of**src-ip6-address** is in dotted hexadecimal notation, in the format of *X:X::X:X*. *M* is an integer in the range 1 to 128. **any** means any source IP address.
dst-ip6-address/M |**any**	Specifies the destination IP address of the designated ACL rule	The value of *src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 128. **any** means any destination IP address.
icmp-type	Specifies the ICMP type range in an ACL rule.	The value is an integer in the range from 0 to 255.
Icmp-code	Specifies the ICMP code range in an ACL rule.	The value is an integer in the range from 0 to 255.

Default Value

None

View

Filter configuration view (IPv6)

Usage Guidelines

None

Example

Configure an ACL rule matching packets based on source and destination IPv6 addresses and the ICMP6 field.

```
switch(configure-filter-ipv6-3500)#filter 100 icmp6 1:1::1:1/10 2:2::2:2/20 100 100
switch(configure-filter-ipv6-3500)#
```

6.3.2 filter igmp6

Function

The **filter igmp6** command configures an ACL rule based on the source/destination IPv6 address and IGMP6 type ID field.

Format

- **filter** *rule-number* **igmp6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** }

Parameters

Parameters	Description	Value
rule-number	Specifies a filter number.	The value is an integer in the range from 1 to 2048.
src-ip6-address/M| **any**	Source IP address of the designated ACL rule	The value of**src-ip6-address** is in dotted hexadecimal notation, in the format of *X:X::X:X. M* is an integer in the range 1 to 128. **any** means any source IP address.
dst-ip6-address/M |**any**	Destination IP address of the designated ACL rule	The value of***dst-ip6-address*** is in dotted hexadecimal notation, in the format of *X:X::X:X. M* is an integer in the range 1 to 128. **any** means any destination IP address.

Default Value

None

View

Filter configuration view (IPv6)

Usage Guidelines

None

Example

Configure an ACL rule based on the source/destination IPv6 address and IGMP6 protocol type field.

```
switch(configure-filter-ipv6-3500)#filter 100 igmp6 1:1::1:1/10 2:2::2:2/20
switch(configure-filter-ipv6-3500)#
```

6.3.3 filter ip6

Function

The **filter ip6** command configures an ACL rule matching packets based on source and destination IPv6 addresses.

Format

- **filter** *rule-number* **ip6** { *src-ip6-address/M* | **any**} { *dst-ip6-address/M* | **any** }

Parameters

Parameters	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer in the range from 1 to 2048.
src-ip6-address/M | **any**	Source IP address of the designated ACL rule	The value of**src-ip6-address** is in dotted hexadecimal notation, in the format of *X:X::X:X*. *M* is an integer in the range 1 to 128. **any** means any source IP address.
dst-ip6-address/M | **any**	Destination IP address of the designated ACL rule	The value of***dst-ip6-address*** is in dotted hexadecimal notation, in the format of *X:X::X:X*. *M* is an integer in the range 1 to 128. **any** means any destination IP address.

View

Filter configuration view (IPv6)

Usage Guidelines

After the ACL entry is applied, a port filters received packets according to the IPv6 addresses in the packets. The port takes the corresponding actions for packets matching the ACL rule.

Warning: The ACL list is classified to four levels:

```
switch(config)#filter-list
  <1-1000>       L2 filter list number
  <1001-2000>    IPv4 filter list number
  <2001-3000>    Hybrid filter list number
  <3001-4000>    IPv6 filter list number
```

The filter ip6 and associated commands are applicable only to IPv6 ACLs 3001 to 4000.

Example

Configure an ACL rule matching packets based on source and destination IPv6 addresses.

```
switch(configure-filter-ipv6-3500)#filter 100 ip6 1:1::1:1/10 2:2::2:2/20
switch(configure-filter-ipv6-3500)#
```

6.3.4 filter ip6 hop-limit

Function

The **filter ip6 hop-limit** command configures an ACL rule based on source and destination IPv6 addresses.

Format

- **filter** *rule-number* **ip6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** } **hop-limit** *hop-value*

Parameters

Parameters	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer in the range from 1 to 2048.
src-ip6-address/M | **any**	Source IP address of the designated ACL rule	The value of**src-ip6-address** is in dotted hexadecimal notation, in the format of *X:X::X:X*. *M* is an integer in the range 1 to 128. **any** means any source IP address.
dst-ip6-address/M | **any**	Destination IP address of the designated ACL rule	The value of***dst-ip6-address*** is in dotted hexadecimal notation, in the format of *X:X::X:X*. *M* is an integer in the range 1 to 128. **any** means any destination IP address.
hop-value	Specifies the hop limit.	The value is an integer in the range from 1 to 255.

View

Filter configuration view (IPv6)

Usage Guidelines

After the ACL entry is applied, a port filters received packets according to the IPv6 addresses in the packets. The port takes the corresponding actions for packets matching the ACL rule, including the limitation on the number of hops in the next packet.

Example

Configure an ACL rule matching packets based on source and destination IPv6 addresses.

```
switch(configure-filter-ipv6-3500)#filter 100 ip6 1:1::1:1/10 2:2::2:2/20 hop-limit 10
switch(configure-filter-ipv6-3500)#
```

6.3.5 filter ip6 next-header

Function

The **filter ip6 next-header** command configures an ACL rule based on source and destination IPv6 addresses.

Format

- **filter** *rule-number* **ip6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** } **next-header** *header-value*

Parameters

Parameters	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer in the range from 1 to 2048.
src-ip6-address/M | **any**	Source IP address of the designated ACL rule	The value of**src-ip6-address** is in dotted hexadecimal notation, in the format of *X:X::X:X*. *M* is an integer in the range 1 to 128. **any** means any source IP address.
dst-ip6-address/M | **any**	Destination IP address of the designated ACL rule	The value of***dst-ip6-address*** is in dotted hexadecimal notation, in the format of *X:X::X:X*. *M* is an integer in the range 1 to 128. **any** means any destination IP address.
header-value	Specifies the value in the next header.	The value is an integer in the range from 1 to 255.

View

Filter configuration view (IPv6)

Usage Guidelines

After the ACL entry is applied, a port filters received packets according to the IPv6 addresses in the packets. The port takes the corresponding actions for packets matching the ACL rule, including the processing of the header value in the next packet.

Example

Configure an ACL rule matching packets based on source and destination IPv6 addresses.

```
switch(configure-filter-ipv6-3500)#filter 100 ip6 1:1::1:1/10 2:2::2:2/20 next-header 10
switch(configure-filter-ipv6-3500)#
```

6.3.6 filter tcp6

Function

The **filter tcp6** command configures an ACL rule matching packets based on source and destination IPv6 addresses and the TCP6 fields (including syn, synack, ack, and fin fields).

Format

- **filter** *rule-number* **tcp6** { *src-ip6-address/M* | **any** } { *source-port-number* | **any** | *source-port-number-range* } { *dst-ip6-address M* | **any** } { *destination-port-number* | **any** | *destination-port-number-range* } { **syn** | **synack** | **ack** | **fin** } [**fragment**]
- **filter** *rule-number* **tcp6** { *src-ip6-address/M* | **any** } { *source-port-number* | **any** | *source-port-number-range* } { *dst-ip6-address M* | **any** } { *destination-port-number* | **any** | *destination-port-number-range* } [**fragment**]

Parameters

Parameters	Description	Value
rule-number	Specifies a filter number.	The value is an integer in the range from 1 to 2048.
src-ip6-address/M| **any**	Specifies the source IP address in an ACL rule.	*src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 128. **any** means any source IP address.
dst-ip6-address/M |**any**	Specifies the destination IP address in an ACL rule.	*src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 128. **any** means any destination IP address.
source-port-number destination-port-number	Specifies the source port number and destination port number.	The value is an integer in the range of <0-65535>.
source-port-number-range destination-port-number-range	Specifies the source port number range and destination port number range.	The value is an integer ranging from 0-65535 / 0-65535.
fragment	Specifies whether the rule is valid for the non-first fragment message only.	-

Default Value

None

View

Filter configuration view (IPv6)

Usage Guidelines

None

Example

Configure an ACL rule matching packets based on source and destination IPv6 addresses and the TCP6 fields (including syn, synack, ack, and fin fields).

```
switch(configure-filter-ipv6-3500)#filter 100 tcp6 1:1::1:1/10 any 2:2::2:2/20 any fragment
switch(configure-filter-ipv6-3500)#
```

6.3.7 filter udp6

Function

The **filter udp6** command configures an ACL rule based on the source/destination IPv6 address and UDP6 field.

Format

- **filter** *rule-number* **udp6** { *src-ip6-address/M* | **any** } { *source-port-number* | **any** | *source-port-number-range* } { *dst-ip6-address M* | **any** } { *destination-port-number* | **any** | *destination-port-number-range* } [**fragment**]

Parameters

Parameters	Description	Value
rule-number	Specifies a filter number.	The value is an integer in the range from 1 to 2048.
src-ip6-address/M| **any**	Source IP address of the designated ACL rule	*src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 128. **any** means any source IP address.
dst-ip6-address/M |**any**	Destination IP address of the designated ACL rule	*src-ip-address* is in the dotted decimal format. *M* is an integer ranging from 1 to 128. **any** means any destination IP address.
source-port-number destination-port-number	Specifies the source port number and destination port number.	The value is an integer in the range of <0-65535>.
source-port-number-range destination-port-number-range	Specifies the source port number range and destination port number range.	The value is an integer ranging from 0-65535 / 0-65535.
fragment	Specifies whether the rule is valid for the non-first fragment message only.	-

Default Value

None

View

Filter configuration view (IPv6)

Usage Guidelines

None

Example

Configure an ACL rule matching packets based on source and destination IPv6 addresses and the UDP6 field.

```
switch(configure-filter-ipv6-3500)#filter 100 udp6 1:1::1:1/10 any 2:2::2:2/20 any fragment
switch(configure-filter-ipv6-3500)#
```

6.4 Traffic Policing and Traffic Shaping Configuration Commands

6.4.1 filter action counter

Function

The **filter action counter** command configures an action in the ACL to count the number of packets based on bytes or packets.

Format

- **filter** *rule-number* **action counter** *counter-number*

Parameters

Parameters	Description	Value
rule-number	Specifies the ACL number.	The value is an integer in the range from 1 to 2048.
counter-number	Specifies the counter number.	The value is an integer in the range from 1 to 1024.

Default Value

None

View

Filter configuration view

Usage Guidelines

After this command is executed, the switch counts the received packets that match the ACL rule based on bytes or packets to calculate the total number of packets passing through the port and matching the ACL rule.

Warning:You must configure the counter in the command of the counter module and bind it with the filter.

```
switch(config)#counter 100 packet sort total
switch(config)#

switch(config)#filter-list 100
switch(configure-filter-l2-100)#
switch(configure-filter-l2-100)#filter 100 mac any any
switch(configure-filter-l2-100)#
```

If different counters are configured, you need to unbind the previously bound counter. Otherwise, the following symptom may occur:

```
switch(configure-filter-l2-100)#filter 100 action counter 200
```

```
%Cannot modify,please release the counter from fliter firstly.
```

Before entering the filter list, enter the ACL. For details, see filter-list.

Example

Configure the action for an ACL rule to statistics collection by bytes or packets.

```
switch(configure-filter-l2-100)#filter 100 action counter 100
switch(configure-filter-l2-100)#
```

6.4.2 filter action mirror group

Function

The **filter action mirror group** command configures an action in the ACL rule to mirror a packet to a specified mirror group.

Format

- **filter** *rule-number* **action mirror group** *group-number*

Parameters

Parameters	Description	Value
rule-number	Specifies the ACL number.	The value is an integer in the range from 1 to 2048.
group-number	Specifies the mirror group number.	The value is an integer in the range from 1 to 7.

Default Value

None

View

Filter configuration view

Usage Guidelines

If this command is used to mirror packets to the specified mirror group, the specified mirror group must have been created. Mirroring process: Upon receiving a packet, the switch performs VLAN, L2, and L3 processing, mirrors the packet to the specified port, and continues to forward the original packet.

Example

Configure the action for an ACL rule to packet mirroring to a specified mirror group.

```
switch(config)#mirror group 1 10gigaethernet 1/0/1
switch(config)#
switch(configure-filter-l2-100)#filter 2 action mirror group 1
switch(configure-filter-l2-100)#
```

Warning: The outgoing direction interface does not support this strategy.

6.4.3 filter meter

Function

The **filter meter** command binds an ACL rule with a meter.
The **no filter meter** command unbinds an ACL rule with a meter.

Format

- **filter** *rule-number* **meter** *meter-number*
- **no filter** *rule-number* **meter**

Parameters

Parameters	Description	Value
rule-number	Specifies an ACL rule number.	The value is an integer in the range from 1 to 2048.
meter-number	Indicates the meter number of a single rate three color packet or two rate three color packet.	The value is an integer in the range from 1 to 256.

Default Value

None

View

Filter configuration view

Usage Guidelines

After this command is executed, the switch limits the rate of a packet matching the ACL rule according to the meter value.

Warning: This command is similar to filter action counter. You must configure the meter in the command of the meter module and bind it with the filter (see meter).

```
switch(config)#meter 100 cir 800 cbs 20000 ebs 20000 aware
switch(config)#

switch(config)#filter-list 100
switch(configure-filter-l2-100)#
switch(configure-filter-l2-100)#filter 100 mac any any
switch(configure-filter-l2-100)#
```

Example

Bind an ACL rule to a meter.

```
switch(configure-filter-l2-100)#filter 100 meter 100
switch(configure-filter-l2-100)#
```

6.4.4 filter action cpu

Function

The **filter action cpu** command sets the action for an ACL rule to CPU forwarding, which means to forward packets matching the rule to the CPU only.

Format

- **filter** *rule-number* **action cpu**

Parameters

Parameters	Description	Value
rule-number	Specifies the ACL number.	The value is an integer in the range from 1 to 2048.
cpu	Indicates that only packets matching the rule are forwarded to the CPU for processing.	-

Default Value

None

View

Filter configuration view

Usage Guidelines

After this command is executed, the switch forwards a packet that matches the ACL rule to the CPU.

Example

Set the action for rule 2 of ACL 100 to CPU forwarding.

```
switch(configure-filter-l2-100)#filter 2 action cpu
switch(configure-filter-l2-100)#
```

6.4.5 filter action {cos|precedence|prioriy}

Function

The**filter action {cos|precedence|priority}** command sets the action in the ACL rule to specify priority of a packet queue passing through a port, modify the three most significant bits in the PRECEDENCE field of the IP packet, and modify the packet priority.

Format

- **filter** *rule-number* **action** { **cos** | **precedence** | **priority** } *priority-value*

Parameters

Parameters	Description	Value
rule-number	Specifies the ACL rule number.	The value is an integer in the range from 1 to 2048.
cos	Specifies the priority of a packet passing through the port queue.	-
precedence	Specifies the three most significant bits in the TOS field of an IP packet.	-
priority	Specifies the packet priority.	The value is an integer in the range from 0 to 7.
priority-value	Specifies the priority value of the COS, PRECEDENCE, and PRIORITY.	The value is an integer in the range from 0 to 7.

Default Value

None

View

Filter configuration view

Usage Guidelines

None

Example

Configure the action in the ACL rule.

```
switch(configure-filter-l2-100)#filter 2 action cos 1
switch(configure-filter-l2-100)#
switch(configure-filter-l2-100)#filter 2 action precedence 2
switch(configure-filter-l2-100)#
```

Warning: The outgoing direction interface does not support this strategy.

6.4.6 filter action dscp

Function

The **filter action dscp** command sets the action for an ACL rule to Differentiated Services Code Point (DSCP) re-marking, which means to change the DSCP field (most significant bits of the ToS field) value of IP packets matching the rule.

Format

- **filter** *rule-number* **action dscp** *dscp-value*

Parameters

Parameters	Description	Value
rule-number	Specifies the ACL number.	The value is an integer in the range from 1 to 2048.
dscp	Specifies the differentiated service code point.	-
Dscp-value	Distinguishes the values of service code points.	The DSCP value is an integer or a name. When the value is an integer, it ranges from 0 to 63. When the value is a name, it is af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, or ef.

Default Value

None

View

Filter configuration view

Usage Guidelines

After this command is executed, the switch changes the DSCP field in a packet that matches the ACL rule to the configured value. For details about Parameters values, see the Parameters description.

Example

Set the action for an ACL rule to DSCP re-marking (changing the value of the six most significant bits of the ToS field) for IP packets matching the rule.

```
switch(configure-filter-l2-100)#filter 2 action dscp 20
switch(configure-filter-l2-100)#
```

6.4.7 filter car outaction drop

Function

The **filter car outaction drop** command sets the action for an ACL rule to dropping excess data packets when the rate of packets exceeds the bandwidth limit of 64 kbit/s x N.

Format

- **filter** *rule-number* **car** *car-value* **outaction drop**

Parameters

Parameters	Description	Value
rule-number	Specifies the ACL number.	The value is an integer in the range from 1 to 2048.

Parameters	Description	Value
car-value	Specifies the multiplier of the bandwidth control granularity (kbit/s).	The value is an integer in the range from 1 to 102400000.

Default Value

None

View

Filter configuration view

Usage Guidelines

After this command is executed, the port determines whether the traffic rate exceeds the limit upon receiving packets matching the ACL rule. If yes, the port drops the packets beyond the traffic limit.

Example

Set the action for an ACL rule to dropping excess data packets when the rate of packets exceeds the bandwidth limit of 64 kbit/s x N.

```
switch(configure-filter-l2-100)#filter 100 car 100 outaction drop
switch(configure-filter-l2-100)#
```

6.4.8 filter outaction

Function

The **filter outaction** command configures the out-action for an ACL rule to dropping packets marked with a single- / dual-rate-three-color marker, re-marking the DSCP priority of IP packets, or re-marking the 802.1p priority of VLAN packets. The **no filter outaction** command deletes the out-action for an ACL rule, which can drop, DSCP re-marking for IP packets, or 802.1p priority re-marking for VLAN packets.

Format

- **filter** *rule-number* **outaction** { **red** | **yellow** } **drop**
- **no filter** *rule-number* **outaction**

Parameters

Parameters	Description	Value
rule-number	Specifies the ACL number.	The value is an integer in the range from 1 to 2048.
red|yellow	Specifies the color marked for a packet.	-
drop	Drops a packet.	-

Default Value

None

View

Filter configuration view

Usage Guidelines

None

Example

Configure the out-action for an ACL rule to dropping packets marked with a single- / dual-rate-three-color marker, re-marking the DSCP priority of IP packets, or re-marking the 802.1p priority of VLAN packets.

```
switch(configure-filter-l2-100)#filter 100 outaction red drop
switch(configure-filter-l2-100)#
```

6.4.9 meter

Function

The **meter** command specifies the CIR, CBS, PIR, EBS, and PBS rate limiting rule through the meter.
The **no meter** command cancels the configuration.

Format

- **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **ebs** *ebs-number*
- **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **ebs** *ebs-number* { **aware** | **blind** }
- **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **pbs** *pbs-number* **pir** *pir-number*
- **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **pbs** *pbs-number* **pir** *pir-number* { **aware** | **blind** }
- **no meter** *meter-number*

Parameters

Parameters	Description	Value
meter-number	Specifies the meter number.	The value is an integer in the range from 1 to 256.
cir-number	Specifies the CIR number.	The value is an integer in the range from 64 to 4294967295.
cbs-number	Specifies the CBS number.	The value is an integer in the range from 10000 to 4294967295.
ebs-number	Specifies the EBS number.	The value is an integer in the range from 10000 to 4294967295.
pbs-number	Specifies the PBS number.	The value is an integer in the range from 10000 to 4294967295.

Parameters	Description	Value
pir-number	Specifies the PIR number.	The value is an integer in the range from 64 to 4294967295.
aware	Indicates the action to respond to the configured rate limiting rule and specified rule.	-
blind	Indicates the action not to respond to the configured rate limiting rule and specified rule.	-

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to configure the QoS CAR template (CIR, CBS, PIR, and PBS), applied to the inbound or outbound interfaces. After the QoS CAR applies to the physical interface or Eth-Trunk interface, the system limits the rate of all upstream packets transmitted over the physical interface or Eth-Trunk interface.
cir-value
The committed information rate (CIR) ensures a mean rate of packets passing through an interface.
The value is an integer in the range from 64 to 4294967295, in kbit/s.
The *cbs-value* specifies the size of the committed burst traffic that can pass through an interface.
The value is an integer ranging from 10000 to 4294967295 in kbit/s.
The pir-value specifies the peak data rate. The value is an integer ranging from 64 to 4294967295. The unit is kbit/s. The pir-value must be equal to or larger than cir-value. By default, pir-value is equal to cir-value. If the pir-value is equal to cir-value, the pbs-value is 0 bytes by default. Otherwise, pbs-value is 125 times pir-value by default.
The pbs-value specifies the size of the peak burst. The value is an integer ranging from 10000 to 4294967295 in kbit . The pbs-value must be equal to or larger than cbs-value.
Traffic-based traffic policing enables a switch to limit the rate of traffic in compliance with the traffic classification rules. By rate limiting, the switch discards traffic beyond the limit, so that traffic entering the switch is limited within a reasonable range, and therefore protecting network resources and carrier's interests. The traffic-based traffic policing adopts the dual-token leaky bucket algorithm.
You can specify the rate limiting rule using the meter, including the CIR, CBS, PIR, and PBS, specify the traffic type through the ACL, and associate the traffic type with the meter. You can enable the ACL at a physical interface (including Trunk) or VLAN interface.
The switch-X supports two types of traffic shaping, namely, port shaping and port queue shaping. You can select the traffic shaping mode according to actual requirements. When both traffic shaping modes co-exist, ensure that the CIR of port shaping is equal to or larger than the sum of CIRs of port queue shaping. Otherwise, traffic shaping is abnormal (for example, traffic in a queue with a lower priority preempts for bandwidth for traffic in a queue with a higher priority).

Example

Specify the CIR, CBS, PIR, EBS, and PBS rate limiting rule using a meter.

```
switch(config)#meter 100 cir 100 cbs 20000 ebs 20000 aware
switch(config)#
```

6.4.10 no filter action

Function

The **no filter action** command deletes the action for an ACL rule.

Format

- **no filter** *rule-number* **action**

Parameters

Parameters	Description	Value
rule-number	Specifies the ACL number.	The value is an integer in the range from 1 to 2048.

Default Value

None

View

Filter configuration view

Usage Guidelines

After using this command, the action corresponding to the ACL rule is deleted.

Example

Delete the action for an ACL rule.

```
switch(configure-filter-l2-100)#no filter 100 action
switch(configure-filter-l2-100)#
```

6.4.11reset counter filter-list

Function

The **reset counter filter-list** command resets the filter count of an ACL.

Format

- **reset counter filter-list** *acl-number* **filter** *rule-number* { **in** | **out** }
- **reset counter filter-list** *acl-number* **filter** *rule-number* **port** { **10gigaethernet** | **100gigaethernet** } *interface-number* { **in** | **out** }
- **reset counter filter-list** *acl-number* **filter** *rule-number* **port eth-trunk** *trunk-number* { **in** | **out** }
- **reset counter filter-list** *acl-number* **filter** *rule-number* **vlan** *vlan-id* { **in** | **out** }

Parameters

Parameters	Description	Value
acl-number	Specifies the ACL number.	The value is an integer ranging from 1 to 4000. <1-1000> specify an L2 ACL. <1001-2000> specify an IPv4 ACL. <2001-3000> specify a hybrid ACL. <3001-4000> specify an IPv6 ACL.
rule-number	Specifies a filter number.	The value is an integer in the range from 1 to 2048.
in|out	Indicates that the ACL takes effect in the inbound or outbound direction of a port.	-
10gigaethernet	Specifies a 10Gigabit Ethernet interface.	-
100gigaethernet	Specifies a 100 Gigabit Ethernet interface.	-
eth-trunk	Specifies an aggregation port.	-
trunk-number	Specifies an aggregation port number.	The value is an integer in the range from 1 to 32.
interface-number	Specifies the port number.	The value is an integer string in the range of <1-1>/<0-2>/<1-52>.
vlan-id	VLAN ID	The value is an integer in the range from 1 to 4094.

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Reset the count of filter 1 in ACL 100 in the inbound direction of GE port 1/0/1.

```
switch(config)#reset counter filter-list 100 filter 1 port 10gigaethernet 1/0/1 in
switch(config)#
```

6.4.12 show meter

Function

The **show meter** command shows rate limiting configuration of the meter, including the CIR, CBS, PIR, EBS, and PBS.

Format

- **show meter**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Show meter configuration.

```
switch#show meter
  ID    CIR       PIR       CBS       EBS       PBS       Mode   Ref-Cnt Status
  1     100       -         100000010000000-          aware 0            Valid
switch#
```

6.4.13 show meter config

Function

The **show meter config** command shows rate limiting configuration of the meter, including the CIR, CBS, PIR, EBS, and PBS.

Format

- **show meter config**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Show meter configuration.

```
switch(config)#show meter config
 Version : METER_VB3.00.00.00
switch(config)#
```

6.5 Queue Scheduling and Congestion Control Configuration Commands

6.5.1 cos priority queue

Function

The **cos priority queue** command sets the priority of a port queue.

Format

- **cos priority** *priority* **queue** { *queue-number* | **default** }

Parameters

Parameters	Description	Value
queue-number	Specifies the queue number.	The value is an integer in the range from 0 to 7.
priority	Priority entry	The value is an integer in the range from 0 to 7.
default	Default Value	1

Default Value

By default, data packets are assigned to queues based on their 802.1p priorities. (If the untagged packets are received, the system specifies an 802.1p priority when adding the PVID to the packets. This 802.1p priority is configurable and default to 1.)

View

Global configuration view

Usage Guidelines

None

Example

Configure the scheduling priority for the port queue.

```
switch(config)#cos priority 1 queue 1
switch(config)#
```

6.5.2 cos queue weight

Function

The **cos queue weight** command sets the weight of queues at an interface.

Format

- **cos queue** *queue-number* **weight** *weight*
- **cos queue** *QUEUE-LIST* **weight** *weight*

Parameters

Parameters	Description	Value
queue-number	Specifies the queue number.	The value is an integer in the range from 0 to 7.
weight	Specifies the weight entry.	The value is an integer in the range from 0 to 15.
QUEUE-LIST	Specifies a queue list.	-

Default Value

If the value is set to the default using the **cos scheduling** command, the switch does not have the default weight entry. If the value is set to WRR using the **cos scheduling** command, the default number of weight entries is 1.

View

Global configuration view

Usage Guidelines

Warning: The cos queue weight command needs to match the cos scheduling algorithm command to complete the configuration (SP+WRR or WRR). If scheduling algorithm is set to SP, you cannot configure cos queue weight. For details, see 6.3.3 cos scheduling.

Example

sets the weight of queues at an interface

```
switch(config)#cos scheduling wrr
switch(config)#cos queue 1 weight 1
switch(config)#
```

6.5.3 cos scheduling

Function

The **cos scheduling** command sets the scheduling mode for queues at an interface.

Format

- **cos scheduling** { **sp** | **rr** | **wrr** }
- **cos scheduling** { **sp+rr** | **sp+wrr** } *QUEUE-LIST*

Parameters

Parameters	Description	Value
sp	Specifies the Strict Priority mode.	-
rr	Specifies the Round Robin.	-
wrr	Specifies the Weighted Round Robin mode.	-
QUEUE-LIST	Specifies a queue list.	-

Default Value

The default mode is SP.

View

Global configuration view

Usage Guidelines

When a network encounters intermittent congestion, congestion management is required if the delay-sensitive services require higher QoS quality than the non-delay-sensitive services. Congestion management is generally implemented using queue scheduling technology. The switch supports the following queue scheduling algorithms:

- SP queue scheduling
- RR queue scheduling
- WRR queue scheduling
- SP + RR queue scheduling
- SP + WRR queue scheduling

Before configuring queue shaping at an interface, set the scheduling mode to WRR for the specified queues. Otherwise, the queue shaping function will not take effect.

Example

#sets the scheduling mode for queues at an interface.

```
switch(config)#cos scheduling sp+rr 1
switch(config)#
```

6.5.4 show cos

Function

The **show cos** command displays the cos queue algorithm and queue information.

Format

- **show cos**

Parameters

None

Default Value

None

View

Common user view, privilege user view, global configuration view, interface configuration view (Ethernet), and interface group configuration view

Usage Guidelines

None

Example

View the cos queue algorithm and queue information.

```
switch#show cos
  scheduling algorithm is sp
  Priority Queue      Weight
  0        0          N/A
  1        1          N/A
  2        2          N/A
  3        3          N/A
  4        4          N/A
  5        5          N/A
  6        6          N/A
  7        7          N/A
switch#
```

6.6 DHCP Snooping Configuration Commands

6.6.1 dhcp-snooping alarm untrust-replay {enable|disable}

Function

The **dhcp-snooping alarm untrust-replay {enable|disable}** command enables or disables an alarm reported when the number of discarded DHCP Reply packets (dropped by the Untrusted port) crosses the threshold.

Format

- **dhcp-snooping alarm untrust-replay** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables an alarm reported when the number of discarded DHCP Reply packets (dropped by the Untrusted port)	-

Parameters	Description	Value
	crosses the threshold.	
disable	Disables an alarm reported when the number of discarded DHCP Reply packets (dropped by the Untrusted port) crosses the threshold.	-

Default Value

disable

View

Interface configuration view (Ethernet and trunk) and interface group configuration view:

Usage Guidelines

None

Example

Enable an alarm reported when the number of discarded DHCP Reply packets (dropped by the Untrusted port) crosses the threshold.

```
switch(config-10ge1/0/1)#dhcp-snooping alarm untrust-reply enable
switch(config-10ge1/0/1)#
```

6.6.2 dhcp-snooping alarm untrust-replay threshold

Function

The **dhcp-snooping alarm untrust-replay threshold** command sets the quantity threshold of the DHCP Reply packets discarded by the port (received by the Untrusted port).

Format

- **dhcp-snooping alarm untrust-replay threshold** { *threshold-value* | **default** }

Parameters

Parameters	Description	Value
threshold-value	Sets the quantity threshold of the DHCP Reply packets (including the Offer, ACK and NAK packets) received by the Untrusted port.	The value is an integer in the range from 1 to 1000.
default	Uses the default threshold.	100

Default Value

100

View

Interface configuration view (Ethernet and trunk) and interface group configuration view:

Usage Guidelines

None

Example

Set the quantity threshold of the DHCP Reply packets discarded by the port (received by the Untrusted port).

```
switch(config-10ge1/0/1)#dhcp-snooping alarm untrust-reply threshold 150
switch(config-10ge1/0/1)#
```

6.6.3 dhcp-snooping binding

Function

The **dhcp-snoop binding** command configures a binding entry.
The **no dhcp-snoop binding** command deletes a binding entry.

Format

- **dhcp-snooping binding** *mac-address ipv4-address vlan-id* { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **dhcp-snooping binding** *mac-address ipv4-address vlan-id* **eth-trunk** *trunk-number*
- **no dhcp-snooping binding** *ipv4-address*
- **no dhcp-snooping binding all**
- **no dhcp-snooping binding interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **no dhcp-snooping binding interface eth-trunk** *trunk-number*
- **no dhcp-snooping binding vlan** *vlan-id*

Parameters

Parameters	Description	Value
mac-address	Specifies the destination MAC address.	The value is in the dotted decimal format, for example, AA:BB:CC:DD:EE:FF, where A-F are decimal numbers ranging from 0 to 255.
ipv4-address	Specifies the destination IPv4 address.	The value is in the dotted decimal format, for example, A.B.C.D, where A-D are decimal numbers in the range from 0 to 255.
vlan-id	Specifies the VID entry.	The value is an integer in the range from 1 to 4094.
trunk-number	Specifies an aggregation port number.	The value is an integer in the range from 1 to 124.
interface-number	Specifies the port number.	The value is an integer string in the range of <1-1>/<0-2>/<1-52>.

Default Value.

None

View

Global configuration view

Usage Guidelines

None

Example

Create a DHCP snooping binding entry.

```
switch(config)#dhcp-snooping binding 11:11:11:11:11:11 2.2.2.2 100 10gigaethernet 1/0/1
switch(config)#
```

6.6.4 dhcp-snooping check mac-address

Function

The **dhcp-snooping check mac-address** command enables or disables the check of MAC addresses in request packets sent from DHCP users.

Format

- **dhcp-snooping check mac-address** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the check of MAC addresses in request packets sent from DHCP users.	-
disable	Disables the check of MAC addresses in request packets sent from DHCP users.	-

Default Value

disable

View

Interface configuration view (Ethernet and trunk), interface group configuration view, VLAN configuration view

Usage Guidelines

None

Example

Enable the check of MAC addresses in request packets sent from DHCP users.

```
switch(config-10ge1/0/1)#dhcp-snooping check mac-address enable
switch(config-10ge1/0/1)#
```

6.6.5 dhcp-snooping check user-bind {enable|disable}

Function

The **dhcp-snooping check user-bind {enable|disable}** command enables or disables the check of DHCP packets against the DHCP binding table.

Format

- **dhcp-snooping check user-bind** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the function of checking whether the DHCP packets match the binding table.	-
disable	Disables the function of checking whether the DHCP packets match the binding table.	-

Default Value

None

View

Interface configuration view (Ethernet and trunk), interface group configuration view, VLAN configuration view

Usage Guidelines

Before running this command, you must run the **dhcp-snooping start** and **dhcp-snooping enable** commands to enable DHCP snooping globally or at an interface.
After this command is executed, the switch checks whether DHCP packets (including DHCP Request and DHCP Reply packets) match the binding table. Checking the Request packets can prevent DHCP lease of illegal users. Checking the Release packets can prevent illegal users from releasing valid IP addresses.

Example

Enable the function of checking whether the DHCP packets match the binding table on interface 10gigaethernet 1/0/1.

```
switch(config)#dhcp-snooping start
switch(config)#interface 10gigaethernet 1/0/1
switch(config-10ge1/0/1)#dhcp-snooping enable
switch(config-10ge1/0/1)#dhcp-snooping check user-bind enable
switch(config-10ge1/0/1)#
```

6.6.6 dhcp-snooping {enable|disable}

Function

The **dhcp-snooping {enable|disable}** command enables or disables DHCP snooping at an interface.

Format

- **dhcp-snooping** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the DHCP Snooping protocol.	-
disable	Disables the DHCP Snooping protocol.	-

Default Value

disable

View

Interface configuration view (Ethernet and trunk), interface group configuration view, VLAN configuration view

Usage Guidelines

None

Example

Enable DHCP snooping at an interface.

```
switch(config-10ge1/0/1)#dhcp-snooping enable
switch(config-10ge1/0/1)#
```

6.6.7 dhcp-snooping max-user-number

Function

The **dhcp-snooping max-user-number** command sets the maximum number of users allowed by each interface.

Format

- **dhcp-snooping max-user-number** { *max-value* | **default** }

Parameters

Parameters	Description	Value
max-value	Specifies the range of the DHCP user quantity.	The value is an integer in the range from 1 to 1024.
default	Indicates the default number of	The Default Value is 1024.

Parameters	Description	Value
	DHCP users.	

Default Value

By default, DHCP snooping allows a maximum of 256 users.

View

Interface configuration view (Ethernet and trunk), interface group configuration view, VLAN configuration view

Usage Guidelines

None

Example

Set the maximum number of users allowed at an interface.

```
switch(config-100ge1/0/1)#dhcp-snooping max-user-number 100
switch(config-100ge1/0/1)#
```

6.6.8 dhcp-snooping option82 circuit-id

Function

The **dhcp-snooping option82 circuit-id** command configures the Circuit-ID content of Option 82.
The **no dhcp-snooping option82 circuit-id** command deletes the Circuit-ID content of Option 82.

Format

- **dhcp-snooping option82 circuit-id** { **ascii** | **hex** } *circuit-id*
- **dhcp-snooping option82 circuit-id ip-address** *ip-address*
- **no dhcp-snooping option82 circuit-id**

Parameters

Parameters	Description	Value
circuit-id	Specifies the circuit ID.	-
ip-address	Specifies the IP address.	The value is in dotted decimal notation.

Default Value

None

View

Interface configuration view (Ethernet and trunk), interface group configuration view, VLAN configuration view

Usage Guidelines

None

Example

Configure the Circuit-ID of Option 82.

```
switch(config-100ge1/0/1)#dhcp-snooping option82 circuit-id ascii "%portname:%svlan.%cvlan%sysname"
switch(config-100ge1/0/1)#
```

6.6.9 dhcp-snooping option82 {circuit-id|remote-id} format

Function

The **dhcp-snooping option82 {circuit-id|remote-id} format** command sets the format of Option 82 sub-option Circuit-ID or Remote-ID to be inserted into DHCP packets at an interface.

Format

- **dhcp-snooping option82 circuit-id format** { **common** | **default** }
- **dhcp-snooping option82 remote-id format** { **common** | **default** }
- **dhcp-snooping option82 circuit-id format user-defined** *txt*
- **dhcp-snooping option82 remote-id format user-defined** *txt*

Parameters

Parameters	Description	Value
circuit-id	Indicates sub-option 1 of Option 82: Circuit-ID (CID).	-
remote-id	Indicates sub-option 2 of Option 82: Remote-ID (RID).	-
common	Indicates the general format of Circuit-ID. Indicates the general format of Remote-ID.	CID format: circuit-id SVLAN (2 bytes)+unit (1 byte)+slot (1 byte)+card (1 byte)+port (1 byte), encapsulated by HEX RID format: remote-id mac (6 bytes), encapsulated by HEX 0 or 6 in the brackets is constantly set to 0 or 6. 2 bytes indicate that the length of the field is 2 bytes.

Parameters	Description	Value
default	Indicates the default format of Circuit-ID. Indicates the default format of Remote-ID.	CID format: circuit-id type (0)+ length (6)+SVLAN (2 bytes)+unit (1 byte)+slot (1 byte)+card (1 byte)+port (1 byte), encapsulated by HEX RID format: remote-id type (0)+length (6)+mac (6 bytes), encapsulated by HEX 0 or 6 in the brackets is constantly set to 0 or 6. 2 bytes indicate that the length of the field is 2 bytes.
user-defined	Customizes the self-defined Option 82 format.	-
txt	Customizes the self-defined Option 82 Circuit-ID or Remote-ID format.	For details about the user-defined format of character strings, see the description in the Command Guidelines.

Default Value

None

View

Interface configuration view (Ethernet and trunk), interface group configuration view, VLAN configuration view

Usage Guidelines

Before using this command, run the **dhco-snooping start** and **dhcp-snooping enable** commands to enable DHCP snooping, and then enable Option 82 on the interface. Otherwise, this command will fail.
The self-defined format character string can contain the following keywords: sysname, portname, porttype, iftype, mac, slot, subslot, port, svlan, and cvlan. For details about the user-defined format character string, see the table below.

Keyword	Meaning
sysname	Specifies the device name.
portname	Specifies the port name.
porttype	Specifies the interface type, which is required when the NAS interface is configured in certain scenarios.
iftype	Specifies the interface type, generally referring to GE, XGE, and Ethernet.
mac	Specifies the MAC address.
slot	Specifies the slot number.

Keyword	Meaning
subslot	Specifies the subslot number.
port	Specifies the port number.
svlan	Specifies the outer VLAN ID.
cvlan	Specifies the inner VLAN ID.

Note: Keywords must be separated by delimiters. Otherwise, the resolution may fail. Therefore, any two keywords must be separated by a non-digit delimiter.

Example

Set the format of Option 82 sub-option Circuit-ID to be inserted to DHCP packets on a interface.

```
switch(config-100ge1/0/1)#dhcp-snooping option82 circuit-id format user-defined %mac
switch(config-100ge1/0/1)#
```

6.6.10 dhcp-snooping option82 {drop|keep|append}

Function

The **dhcp-snooping option82 {drop|keep|append}** command sets the policy for the Option 82 field in DHCP packets.

Format

- **dhcp-snooping option82** { **drop** | **keep** | **append** }

Parameters

Parameters	Description	Value
(drop|keep|append)	Option 82 policies, including discarding, keeping and adding policies	-

Default Value

The default policy is keep.

View

Interface configuration view (Ethernet and trunk), interface group configuration view, VLAN configuration view

Usage Guidelines

None

Example

Configure the policy for the Option 82 field in DHCP packets.

```
switch(config-100ge1/0/1)#dhcp-snooping option82 drop
```

```
switch(config-100ge1/0/1)#
switch(config-100ge1/0/1)#dhcp-snooping option82 keep
switch(config-100ge1/0/1)#
switch(config-100ge1/0/1)#dhcp-snooping option82 append
switch(config-100ge1/0/1)#
```

6.6.11dhcp-snooping option82 {enable|disable}

Function

The **dhcp-snooping option82 {enable|disable}** command enables or disables Option 82 insertion to DHCP Request packets at an interface.

Format

- **dhcp-snooping option82** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables Option 82 insertion to DCHP Request packets at an interface.	-
disable	Disables Option 82 insertion to DCHP Request packets at an interface.	-

Default Value

None

View

Interface configuration view (Ethernet and trunk), interface group configuration view, VLAN configuration view

Usage Guidelines

None

Example

Enable Option 82 insertion to DCHP Request packets at an interface.

```
switch(config-100ge1/0/1)#dhcp-snooping option82 enable
switch(config-100ge1/0/1)#
```

6.6.12 dhcp-snooping option82 remote-id

Function

The **dhcp-snooping option82 remote-id** command configures the Remote-ID content of Option 82.
The **no dhcp-snooping option82 remote-id** command deletes the Remote-ID content of Option 82.

Format

- **dhcp-snooping option82 remote-id** { **ascii** | **hex** } *remote-id*
- **dhcp-snooping option82 remote-id ip-address** *ip-address*
- **no dhcp-snooping option82 remote-id**

Parameters

Parameters	Description	Value
remote-id	Specifies the Remote ID.	-
ip-address	Specifies the IP address.	The value is in dotted decimal notation.

Default Value

None

View

Interface configuration view (Ethernet and trunk), interface group configuration view, VLAN configuration view

Usage Guidelines

None

Example

Configure the Remote-ID of Option 82.

```
switch(config-100ge1/0/1)#dhcp-snooping option82 remote-id ascii 2
switch(config-100ge1/0/1)#
```

6.6.13 dhcp-snooping option82 sub-option9

Function

The **dhcp-snooping option82 sub-option9 {enable|disable}** command enables or disables sub-option 9 of Option 82 at an interface.
The **dhcp-snooping option82 sub-option9** command sets the sub-option 9 content of Option 82.
The **no dhcp-snooping option82 sub-option9** command deletes the sub-option 9 content of Option 82.

Format

- **dhcp-snooping option82 sub-option9** { **enable** | **disable** }
- **dhcp-snooping option82 sub-option9** *string*
- **no dhcp-snooping option82 sub-option9**

Parameters

Parameters	Description	Value
string	Specifies the sub-option 9 entry.	-

Default Value

By default, Option 82 will be added to DHCP packets at an interface if DHCP snooping Option 82 is enabled on the interface. By default, sub-option 9 will not be added to Option 82 unless the **dhcpsnoop option82 sub-option9 enable** command is configured.

View

Interface configuration view (Ethernet and trunk), interface group configuration view, VLAN configuration view

Usage Guidelines

By default, the sub-option 9 is set to the enterprise number + hostname. You can also configure it using this command to fill the content following the enterprise number in sub-option 9.

Example

Enables sub-option 9 of Option 82 at an interface.

```
switch(config-100ge1/0/1)#dhcp-snooping option82 sub-option9 enable
switch(config-100ge1/0/1)#
```

6.6.14 dhcp-snooping relay server-ip

Function

The **dhcp-snooping relay server-ip** command configures the IP address of the DHCP Snooping relay server.
The **no dhcp-snooping relay server-ip** command deletes the IP address of the DHCP Snooping relay server.

Format

- **dhcp-snooping relay server-ip** *ip-address*
- **no dhcp-snooping relay server-ip** *ip-address*

Parameters

Parameters	Description	Value
ip-address	Specifies the IP address of the relay server.	The value is in dotted decimal notation.

Default Value

None

View

Interface configuration view (Ethernet and trunk) and interface group configuration view:

Usage Guidelines

Before using this command, you must run the dhcp-snooping start and dhcp-snooping enable commands to enable DHCP Snooping. Otherwise, this command fails.

Example

Configure the IP address of the DHCP snooping relay server.

```
switch(config)#dhcp-snooping start
switch(config)#interface 10gigaethernet 1/0/1
switch(config-100ge1/0/1)#dhcp-snooping enable
switch(config-100ge1/0/1)#dhcp-snooping relay server-ip 1.1.1.1
switch(config-100ge1/0/1)#
```

6.6.15 dhcp-snooping relay-agent-ip

Function

The **dhcp-snooping relay-agent-ip** command configures the IP address of the DHCP Snooping relay proxy.
The **no dhcp-snooping relay-agent-ip** command deletes the IP address of the DHCP Snooping relay proxy.

Format

- **dhcp-snooping relay-agent-ip** *ip-address*
- **no dhcp-snooping relay-agent-ip**

Parameters

Parameters	Description	Value
ip-address	Specifies the IP address of the relay proxy.	The value is in dotted decimal notation.

Default Value

None

View

Interface configuration view (Ethernet and trunk) and interface group configuration view:

Usage Guidelines

Before using this command, you must run the dhcp-snooping start and dhcp-snooping enable commands to enable DHCP Snooping. Otherwise, this command fails.

Example

Configure the IP address of the DHCP snooping relay server.

```
switch(config)#dhcp-snooping start
switch(config)#interface 100gigaethernet 1/0/1
switch(config-100ge1/0/1)#dhcp-snooping enable
switch(config-100ge1/0/1)#dhcp-snooping relay-agent-ip 2.1.1.1
switch(config-100ge1/0/1)#
```

6.6.16 dhcp-snooping sticky-mac {enable|disable}

Function

The **dhcp-snooping sticky-mac {enable|disable}** command enables or disables the generation of static MAC table entries based on DHCP Snooping dynamic binding table.

Format

- **dhcp-snooping sticky-mac** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the generation of static MAC table entries based on DHCP Snooping dynamic binding table.	-
disable	Disables the generation of static MAC table entries based on DHCP Snooping dynamic binding table.	-

Default Value

disable

View

Interface configuration view (Ethernet and trunk) and interface group configuration view:

Usage Guidelines

None

Example

Enable the generation of static MAC table entries based on DHCP Snooping dynamic binding table.

```
switch(config-100ge1/0/1)#dhcp-snooping sticky-mac enable
switch(config-100ge1/0/1)#
```

6.6.17 dhcp-snooping server detect

Function

The **dhcp-snooping server detect** command enables or disables detection of pseudo DHCP snooping servers.

Format

- **dhcp-snooping server detect** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables detection of pseudo DHCP Snooping servers.	-

Parameters	Description	Value
disable	Disables detection of pseudo DHCP Snooping servers.	-

Default Value

By default, detection of pseudo DHCP Snooping servers is disabled.

View

Global configuration view

Usage Guidelines

None

Example

Enable detection of pseudo DHCP Snooping servers.

```
switch(config)#dhcp-snooping server detect enable
switch(config)#
```

6.6.18 dhcp-snooping {start|stop}

Function

The **dhcp-snooping {start|stop}** command enables or disables DHCP snooping globally.

Format

- **dhcp-snooping** { **start** | **stop** }

Parameters

Parameters	Description	Value
start	Enables DHCP Snooping.	-
stop	Disables DHCP Snooping.	-

Default Value

disable

View

Global configuration view

Usage Guidelines

None

Example

Enable the DHCP snooping protocol globally.

```
switch(config)#dhcp-snooping start
switch(config)#
```

6.6.19 dhcp-snooping {trust|untrust}

Function

The **dhcp-snooping {trust|untrust}** command configures an interface as a trusted or untrusted interface.

Format

- **dhcp-snooping** { **trust** | **untrust** }

Parameters

Parameters	Description	Value
trust	Indicates a trusted interface.	-
untrust	Indicates an untrusted interface.	-

Default Value

None

View

Interface configuration view (Ethernet and trunk) and interface group configuration view:

Usage Guidelines

None

Example

Configure an interface as a trusted interface.

```
switch(config-100ge1/0/1)#dhcp-snooping trust
switch(config-100ge1/0/1)#
```

6.6.20 dhcp-snooping trust interface

Function

The **dhcp-snooping trust interface** command configures the DHCP snooping trust interface based on VLAN.

Format

- **dhcp-snooping trust interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **dhcp-snooping trust interface eth-trunk** *trunk-number*

- **no dhcp-snooping trust interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **no dhcp-snooping trust interface eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of 1-1/0-2/1-52.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 124.

Default Value

None

View

VLAN configuration view

Usage Guidelines

None

Example

Configure the DHCP snooping trust interface based on VLAN.

```
switch(config)#dhcp-snooping start
switch(config)#vlan 1
switch (vlanif-1)#dhcp-snooping enable
switch (vlanif-1)#dhcp-snooping trust interface 10gigaethernet 1/0/1
```

6.6.21 reset dhcp-snooping statistic

Function

The **reset dhcp-snooping statistic** command resets DHCP snooping statistics.

Format

- **reset dhcp-snooping statistic**

Parameters

None

Default Value

None

View

Global configuration view, interface configuration view (Ethernet and trunk), interface group configuration view, VLAN configuration view

Usage Guidelines

None

Example

Reset global DHCP snooping statistics.

```
switch(config)#reset dhcp-snooping statistic
switch(config)#
```

6.6.22 show dhcp-snooping binding

Function

The **show dhcp-snooping binding** command displays DHCP snooping user binding configuration.

Format

- **show dhcp-snooping binding**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), interface group configuration view, and VLAN configuration view

Usage Guidelines

The information includes IP-Addr, Mac-Addr, Vlan, Interface, Time, AgeTime, and State.

Example

Display DHCP snooping user binding configuration.

```
switch(config-100ge1/0/1)#show dhcp-snooping binding
Total Number:1
IP-Addr        Mac-Addr           Vlan   Interface     Time          AgeTime       State
2.2.2.2     11:11:11:11:11:11     100     100ge-1/0/1     unlimited          2          static


switch(config-100ge1/0/1)#
```

6.6.23 show dhcp-snooping config

Function

The **show dhcp-snooping config** command displays DHCP snooping configuration.

Format

- **show dhcp-snooping config**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), interface group configuration view, and VLAN configuration view

Usage Guidelines

The information includes dhcp-snooping start and dhcp-snooping binding.

Example

Display DHCP snooping configuration.

```
switch(config-100ge1/0/1)#show dhcp-snooping config
 Version:DHCPSNOOP_VB3.00.03.00
 dhcp-snooping start
 interface 100gigaethernet 1/0/1
 dhcp-snooping enable
 dhcp-snooping relay-agent-ip 2.1.1.1
 dhcp-snooping relay server-ip 1.1.1.1
switch(config-100ge1/0/1)#
```

6.6.24 show dhcp-snooping fake-server

Function

The **show dhcp-snooping fake-server** command displays fake DHCP server information.

Format

- **show dhcp-snooping fake-server**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Display the fake DHCP server information.

```
switch#show dhcp-snooping fake-server
IpAddr                Vid          Interface
12.1.1.2              1            100ge-1/0/2
switch#
```

6.6.25 show dhcp-snooping interface

Function

The **show dhcp-snooping interface** command displays DHCP snooping interface configuration.

Format

- **show dhcp-snooping interface**
- **show dhcp-snooping interface** { **10gigaethernet** | **10gigaethernet** } *interface-number*
- **show dhcp-snooping interface eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer string in the range of <1-1>/<0-2>/<1-52>.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), interface group configuration view, and VLAN configuration view

Usage Guidelines

The information includes the specific interface information and global interface information.

Example

Display DHCP snooping interface configuration.

```
switch(config)#show dhcp-snooping interface
Interface     Status   Version Trust     Dynamic User Number
100ge-1/0/1       enable   v4          untrust 0

switch(config)#show dhcp-snooping interface 100gigaethernet 1/0/1
 dhcp-snooping enable
 dhcp-snooping relay-agent-ip 2.1.1.1
 dhcp-snooping relay server-ip 1.1.1.1
switch(config)#
```

6.6.26 show dhcp-snooping statistic

Function

The **show dhcp-snooping statistic** command displays DHCP snooping interface statistics.

Format

- **show dhcp-snooping statistic**
- **show dhcp-snooping statistic interface** { **10gigaethernet | 100gigaethernet** } *interface-number*
- **show dhcp-snooping statistic interface eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer string in the range of <1-1>/<0-2>/<1-52>.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), interface group configuration view, and VLAN configuration view

Usage Guidelines

The information includes specific interface information and global interface information. The global interface information includes Source mac mismatch, Binding entry mismatch, Untrust reply received, Discord ARP, Discord IP, and Discord DHCP.

Example

Display DHCP snooping interface statistics.

```
switch(config)#show dhcp-snooping statistic
Interface : 10ge-1/0/1
 Source mac mismatch : 0
 Binding entry mismatch : 0
 Untrust reply received : 0
 Discord ARP : 0
 Discord IP : 0
 Discord DHCP : 0
switch(config)#show dhcp-snooping statistic interface 10gigaethernet 1/0/1
Interface : 10ge-1/0/1
 Source mac mismatch : 0
 Binding entry mismatch : 0
 Untrust reply received : 0
 Discord ARP : 0
 Discord IP : 0
 Discord DHCP : 0
switch(config)#
```

6.7 IP Source Guard Configuration Commands

6.7.1 ip source check user-bind {enable|disable}

Function

The **ip source check user-bind enable** command enables the IP packet check function at an interface.
The **ip source check user-bind disable** command disables the IP packet check function at an interface.

Format

- **ip source check user-bind enable**
- **ip source check user-bind disable**

Parameters

None

Default Value

By default, the switch does not check whether an IP packet matches the binding table.

View

Interface configuration view (Ethernet and trunk) and interface group configuration view:

Usage Guidelines

You can use this command to check IP packets match a binding table and determine whether a switch is allowed to forward the packets.
To prevent IP packets of illegal users from accessing the external network through the switch, you can enable the IP packet check function at an interface. Only IP packets matching the binding table can be forwarded.
For a DHCP user, a dynamic binding table is generated after DHCP Snooping is enabled.
For a static address user, you need to manually establish the static binding table.

Example

Enable the IP packet check function at an interface.

```
switch(config-100ge1/0/1)#ip source check user-bind enable
switch(config-100ge1/0/1)#
```

6.7.2 ip source check user-bind alarm {enable|disable}

Function

The **ip source check user-bind alarm {enable|disable}** command enables or disables the alarm for IP packet check.

Format

- **ip source check user-bind alarm** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the alarm for IP packet check.	-
disable	Disables the alarm for IP packet check.	-

Default Value

disable

View

Interface configuration view (Ethernet and trunk) and interface group configuration view:

Usage Guidelines

None

Example

Enable the alarm function for IP packet check.

```
switch(config-100ge1/0/1)#ip source check user-bind enable
switch(config-100ge1/0/1)#ip source check user-bind alarm enable
switch(config-100ge1/0/1)#
```

6.7.3 ip source check user-bind alarm threshold

Function

The **ip source check user-bind alarm threshold** command sets the alarm threshold for IP packet check.

Format

- **ip source check user-bind alarm threshold** { *value* | **default** }

Parameters

Parameters	Description	Value
value	Specifies the alarm threshold for IP packet check.	The value is an integer in the range from 1 to 1000.
default	Uses the default threshold.	100

Default Value

100

View

Interface configuration view (Ethernet and trunk) and interface group configuration view:

Usage Guidelines

None

Example

Set the alarm threshold for IP packet check.

```
switch(config-100ge1/0/1)#ip source check user-bind enable
switch(config-100ge1/0/1)#ip source check user-bind alarm threshold 200
switch(config-100ge1/0/1)#
```

6.7.4 ip source check user-bind check-item

Function

The **ip source check user-bind check-item** command sets the item for IP packet check.
The **no ip source check user-bind check-item** command restores the item for IP packet check to the default option.

Format

Interface configuration view:

- **ip source check user-bind check-item** { **ip-address** | **mac-address** | **vlan** }
- **ip source check user-bind check-item ip-address mac-address**
- **ip source check user-bind check-item ip-address vlan**
- **ip source check user-bind check-item mac-address vlan**
- **no ip source check user-bind check-item**

VLAN configuration view:

- **ip source check user-bind check-item** { **ip-address** | **mac-address** | **interface** }
- **ip source check user-bind check-item ip-address interface**
- **ip source check user-bind check-item ip-address mac-address**
- **ip source check user-bind check-item mac-address interface**
- **no ip source check user-bind check-item**

Parameters

Parameters	Description	Value
ip-address	Checks whether the IPv4 address of an IP packet matches the binding table.	-
mac-address	Checks whether the MAC address of an IP packet matches the binding table.	-
vlan	Checks whether the VLAN of an IP packet matches the binding table.	-
interface	Checks whether the interface of an IP packet matches the binding table.	-

Default Value

By default, the system checks the IP addresses, MAC addresses, and VLANs of IP packets.

View

Interface configuration view (Ethernet and trunk), interface group configuration view, VLAN configuration view

Usage Guidelines

None

Example

Enable the IP Source Guard at an interface and check whether the VLAN of an IP packet matches a binding table.

```
switch(config-100ge1/0/1)#ip source check user-bind enable
switch(config-100ge1/0/1)#ip source check user-bind check-item vlan
switch(config-100ge1/0/1)#
```

6.7.5 reset ip source statistic check user-bind

Function

The **reset ip source statistic check user-bind** command clears the IP Source Guard statistics.

Format

- **reset ip source statistic check user-bind**

Parameters

None

Default Value

None

View

Interface configuration view (Ethernet and trunk) and interface group configuration view

Usage Guidelines

None

Example

Clear the IP Source Guard statistics.

```
switch(config-100ge1/0/1)#ip source check user-bind enable
switch(config-100ge1/0/1)#reset ip source statistic check user-bind
switch(config-100ge1/0/1)#
```

6.7.6 show ip source check user-bind

Function

The **show ip source check user-bind** command shows information of the IP packet checking function.

Format

- **show ip source check user-bind**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

None

Example

Display information of the IP packet checking function.

```
switch#show ip source check user-bind

 interface 10gigaethernet 1/0/1
 ip source check user-bind enable
 ip source check dropped IP packets 0/0
switch#
```

6.7.7 show user-bind

Function

The **show user-bind** command shows the information of the static binding entry.

Format

- **show user-bind**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

None

Example

View the information of the static binding entry.

```
switch(config)#user-bind static ip 10.1.1.1 mac 01:01:01:01:01:01 interface 10gigaethernet 1/0/1 vlan 1

 switch(config)#show user-bind
 1 entries in user-bind table
Interface            IP-Address      Mac-Address       Vlan      Type
10ge-1/0/1           10.1.1.1        01:01:01:01:01:01 1         IPSG
switch(config)#
```

6.7.8 show user-bind config

Function

The **show user-bind config** command shows the configuration of the static binding entry.

Format

- **show user-bind config**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

None

Example

View the configuration of the static binding entry.

```
switch(config)#show user-bind config
user-bind static ip 10.1.1.1 mac 01:01:01:01:01:01 interface 10gigaethernet 1/0/1 vlan 1
switch(config)#
```

6.7.9 user-bind alarm untrust-user

Function

The **user-bind alarm untrust-user {enable|disable}** command enables or disables the alarm for untrusted IP packets received.
The **user-bind alarm untrust-user threshold** command configures the threshold for untrusted IP packets received.

Format

- **user-bind alarm untrust-user** { **enable** | **disable** }
- **user-bind alarm untrust-user threshold** { *threshold* | **default** }

Parameters

Parameters	Description	Value
enable	Enables the alarm for IP packet check.	-

Parameters	Description	Value
disable	Disables the alarm for IP packet check.	-
threshold	Sets the IP packet checking alarm threshold.	The value is an integer ranging from 1 to 1000.
default	Indicates default IP packet checking alarm threshold	100

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Enable the alarm function for IP packet check.

```
switch(config)#user-bind alarm untrust-user enable
switch(config)#
```

6.7.10 user-bind black-list

Function

The **user-bind black-list** command enables or disables the IP packet blacklist.

Format

- **user-bind black-list** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the IP packet blacklist.	-
disable	Disables the IP packet blacklist.	-

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Enable the IP packet blacklist.

```
switch(config)#user-bind black-list enable
switch(config)#
```

6.7.11user-bind static ip|ip6 mac

Function

The **user-bind static ip|ip6 mac** command configures static binding entries.
The **no user-bind static** command deletes static binding entries.

Format

- **user-bind static ip** { *ipv4-address* | **any** } **mac** { *src-mac-address* | **any** } **interface** { **10gigaethernet** | **100gigaethernet** } *interface-number* **vlan** { **any** | *vlan-id* }
- **user-bind static ip** { *ipv4-address* | **any** } **mac** { *src-mac-address* | **any** } **vlan** { **any** | *vlan-id* }
- **user-bind static ip6** { *ipv6-address* | **any** } **mac** { *src-mac-address* | **any** } **interface** { **10gigaethernet** | **100gigaethernet** } *interface-number* **vlan** { **any** | *vlan-id* }
- **user-bind static ip6** { *ipv6-address* | **any** } **mac** { *src-mac-address* | **any** } **vlan** { **any** | *vlan-id* }
- **no user-bind static ip** { *ipv4-address* | **any** } **mac** { *src-mac-address*| **any** } **interface** { **10gigaethernet** | **100gigaethernet** } *interface-number* **vlan** { **any** | *vlan-id* }
- **no user-bind static ip** { *ipv4-address* | **any** } **mac** { *src-mac-address* | **any** } **vlan** { **any** | *vlan-id* }
- **no user-bind static ip6** { *ipv6-address* | **any** } **mac** { *src-mac-address*| **any** } **interface** { **10gigaethernet** | **100gigaethernet** } *interface-number* **vlan** { **any** | *vlan-id* }
- **no user-bind static ip6** { *ipv6-address* | **any** } **mac** { *src-mac-address* | **any** } **vlan** { **any** | *vlan-id* }
- **no user-bind static all**
- **no user-bind static interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **no user-bind static ip** *ipv4-address*
- **no user-bind static ip6** *ipv6-address*
- **no user-bind static mac** *src-mac-address*
- **no user-bind static vlan** *vlan-id*

Parameters

Parameters	Description	Value
ipv4-address	Specifies the source IPv4 address.	The value is in the dotted decimal format, for example, A.B.C.D, where A-D are decimal numbers in the range from 0 to 255.
ipv6-address	Specifies the source IPv6 address.	-
src-mac-address | **any**	Specifies the source MAC	The value is hexadecimal.

Parameters	Description	Value
	address in an ACL rule.	The field **any** means any source MAC address.
any | vlan-id	The field **any** indicates that the Parameters is not matched. *vlan-id* indicates the VID entry to which the user belongs.	The value is an integer in the range from 1 to 4094. The field **any** means any VID.
interface-number	Specifies an Ethernet interface number.	The value is an integer string in the range of <1-1>/<0-2>/<1-52>.

Uses the Default Value.

None

View

Global configuration view

Usage Guidelines

None

Example

Configure a static binding entry.

```
switch(config)#user-bind static ip 10.1.1.1 mac 01:01:01:01:01:01 interface 10gigaethernet 1/0/1 vlan 1
switch(config)#
```

6.8 AAA/Radius Configuration Commands

6.8.1 aaa

Function

The **aaa** command is used to switch to the AAA configuration view from the global configuration view.

Format

- **aaa**

Parameters

None

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Switch to the AAA configuration view from the global configuration view.

```
switch(config)#aaa
switch(config-aaa)#
```

6.8.2 aaa authorization console

Function

The **aaa authorization console** command enables the console to use AAA authorization.
The **no aaa authorization console** command disables the console to use AAA authorization.

Format

- **aaa authorization console**
- **no aaa authorization console**

Parameters

None

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Enable the console to use AAA authorization.

```
switch(config)#aaa authorization console
switch(config)#
```

6.8.3 aaa {authentication|account}

Function

The **aaa {authentication|account}** command configures the AAA authentication name or AAA accounting name.

Format

- **aaa** { **authentication** | **account** } { **dot1x** | **ppp** | **login** | **web-auth** | **mac-authen** } **method** *name* **server-group** *group-name*
- **aaa** { **authentication** | **account** } { **dot1x** | **ppp** | **login** | **web-auth** | **mac-authen** } **method** *name* **server-group** *group-name* { **local** | **none** }
- **aaa** { **authentication** | **account** } { **dot1x** | **ppp** | **login** | **web-auth** | **mac-authen** } **method** *name* **server-group** *group-name* **local none**
- **aaa** { **authentication** | **account** } { **dot1x** | **ppp** | **login** | **web-auth** | **mac-authen** } **method** *name* **server-group** *group-name group-name*
- **aaa** { **authentication** | **account** } { **dot1x** | **ppp** | **login** | **web-auth** | **mac-authen** } **method** *name* **server-group** *group-name group-name* { **local** | **none** }
- **aaa** { **authentication** | **account** } { **dot1x** | **ppp** | **login** | **web-auth** | **mac-authen** } **method** *name* **server-group** *group-name group-name* **local none**
- **aaa** { **authentication** | **account** } { **dot1x** | **ppp** | **login** | **web-auth** | **mac-authen** } **local method** *name* **server-group** *group-name*
- **aaa** { **authentication** | **account** } { **dot1x** | **ppp** | **login** | **web-auth** | **mac-authen** } **local method** *name* **server-group** *group-name group-name*
- **aaa** { **authentication** | **account** } { **dot1x** | **ppp** | **login** | **web-auth** | **mac-authen** } **local method** *name* **server-group** *group-name group-name* **none**
- **aaa** { **authentication** | **account** } { **dot1x** | **ppp** | **login** | **web-auth** | **mac-authen** } **local method** *name* **server-group** *group-name* **none**
- **aaa authentication** { **dot1x** | **ppp** | **login** | **web-auth** | **mac-authen** } **method** *name* **local**
- **aaa authentication** { **dot1x** | **ppp** | **login** | **web-auth** | **mac-authen** } **local method** *name*

Parameters

Parameters	Description	Value
authentication	Specifies the authentication.	-
account	Specifies the accounting.	-
dot1x	Specifies the IEEE 802.1X protocol.	-
ppp	Specifies the point-to-point protocol.	-
login	Specifies the login authentication.	-
web-auth	Specifies the Web authentication.	-
mac-authen	Specifies the MAC address authentication.	-
name	Specifies the method list name.	The value is a character string.
group-name	Specifies the server group name.	The value is a character string.
local	Enables local authentication.	-
none	Disables authentication or accounting.	-

Default Value

None

View

AAA configuration view

Usage Guidelines

None

Example

Configure an AAA authentication method name or AAA accounting method name.

```
switch(config-aaa)#aaa authentication login method 11 server-group test
switch(config-aaa)#aaa account login method 11 server-group aaa bbb
switch(config-aaa)#
```

6.8.4 aaa authentication enable method

Function

The **aaa authentication enable method** command creates the aaa enable (secondary authentication) method.

Format

- **aaa authentication enable method** *name* **local**
- **aaa authentication enable method** *name* **server-group** *group-name*
- **aaa authentication enable method** *name* **server-group** *group-name* { **local** | **none** }
- **aaa authentication enable method** *name* **server-group** *group-name group-name*
- **aaa authentication enable method** *name* **server-group** *group-name group-name* { **local** | **none** }
- **aaa authentication enable method** *name* **server-group** *group-name group-name* **local none**
- **aaa authentication enable method** *name* **server-group** *group-name* **local none**
- **aaa authentication enable local method** *name*
- **aaa authentication enable local method** *name* **server-group** *group-name*
- **aaa authentication enable local method** *name* **server-group** *group-name group-name*
- **aaa authentication enable local method** *name* **server-group** *group-name group-name* **none**
- **aaa authentication enable local method** *name* **server-group** *group-name* **none**

Parameters

Parameters	Description	Value
name	Specifies the method list name.	The value is a character string.
group-name	Specifies the server group name.	The value is a character string.
local	Enables local authentication.	-
none	Disables authentication.	-

Default Value

None

View

AAA configuration view

Usage Guidelines

None

Example

Create a secondary authentication method.

```
switch(config-aaa)#aaa authentication enable method 11 local
switch(config-aaa)#
```

6.8.5 aaa authorization method

Function

The **aaa authorization method** command creates the AAA authorization method.

Format

- **aaa authorization method** *name* **local**
- **aaa authorization method** *name* **server-group** *group-name*
- **aaa authorization method** *name* **server-group** *group-name* { **local** | **none** }
- **aaa authorization method** *name* **server-group** *group-name group-name*
- **aaa authorization method** *name* **server-group** *group-name group-name* { **local** | **none** }
- **aaa authorization method** *name* **server-group** *group-name group-name* **local none**
- **aaa authorization method** *name* **server-group** *group-name* **local none**

Parameters

Parameters	Description	Value
name	Specifies the method list name.	The value is a character string.
group-name	Specifies the server group name.	The value is a character string.
local	Enables local authentication.	-
none	Disables authentication.	-

Default Value

None

View

AAA configuration view

Usage Guidelines

None

Example

Create an AAA authorization method.

```
switch(config-aaa)#aaa authorization method 11 local
switch(config-aaa)#
```

6.8.6 account realtime

Function

The **account realtime** command sets the AAA real-time accounting report interval.

Format

- **account realtime** { *realtime* | **default** }

Parameters

Parameters	Description	Value
realtime	Indicates the failure time.	The value is an integer in the range from 300 to 4294967290 (unit: s).
default	Indicates the default.	The default is 300.

Default Value

300 seconds

View

AAA configuration view

Usage Guidelines

None

Example

Set the AAA real-time accounting report interval.

```
switch(config-aaa)#account realtime 1000
switch(config-aaa)#
```

6.8.7 no aaa method

Function

The **no aaa method** command deletes an AAA method or deletes the server group in the AAA method.

Format

- **no aaa method** *name*
- **no aaa method** *name* **server-group** *group-name*

Parameters

Parameters	Description	Value
name	Specifies an AAA method name	The value is a character string.
group-name	Specifies the server group name.	The value is a character string.

Default Value

None

View

AAA configuration view

Usage Guidelines

None

Example

Delete an AAA method or a server group from an AAA method.

```
switch(config-aaa)#no aaa method 11
switch(config-aaa)#
switch(config-aaa)#no aaa method 11 server-group aaa
switch(config-aaa)#
```

6.8.8 no radius-server

Function

The **no radius-server** command deletes an AAA RADIUS server.

Format

- **no radius-server** *name*
- **no radius-server** *name* **src-ip**
- **no radius-server** *name* **src-ipv6**

Parameters

Parameters	Description	Value
name	Specifies the RADIUS server name.	The value is a character string.

Default Value

None

View

AAA configuration view

Usage Guidelines

None

Example

Delete an AAA RADIUS server.

```
switch(config-aaa)#no radius-server 111
switch(config-aaa)#
```

6.8.9 no server-group

Function

The **no server-group** command deletes an AAA server group or deletes a server from the AAA server group.

Format

- **no aaa server-group** *name*
- **no aaa server-group** *name* **radius-server** *server-name*
- **no aaa server-group** *name* **tacacs-server** *server-name*

Parameters

Parameters	Description	Value
name	Specifies the server group name.	The value is a character string.
server-name	Specifies the RADIUS server name.	The value is a character string.

Default Value

None

View

AAA configuration view

Usage Guidelines

None

Example

Delete a server from the AAA server group.

```
switch(config-aaa)#no aaa server-group group1 radius-server ccc
switch(config-aaa)#
```

6.8.10 no tacacs-server

Function

The **no tacacs-server** command deletes a TACACS server.

Format

- **no tacacs-server** *name*
- **no tacacs-server** *name* **src-ip**
- **no tacacs-server** *name* **src-ipv6**

Parameters

Parameters	Description	Value
name	Specifies the Tacacs server name.	The value is a character string.

Default Value

None

View

AAA configuration view

Usage Guidelines

None

Example

Delete a TACACS server.

```
switch(config-aaa)#no tacacs-server feisu
switch(config-aaa)#
```

6.8.11radius-server acct-port

Function

The **radius-server acc-port** command configures the accounting port for a RADIUS server.

Format

- **radius-server** *name* **acc-port** { *acc-port* | **default** }

Parameters

Parameters	Description	Value
name	Specifies the RADIUS server name.	The value is a character string.
acc-port	Specifies the accounting port number.	The value is an integer in the range from 1 to 65535.
default	Default Value	1813

Default Value

1813

View

AAA configuration view

Usage Guidelines

None

Example

Configure an accounting port for a RADIUS server.

```
switch(config-aaa)#radius-server 111 acct-port 100
switch(config-aaa)#
```

6.8.12 radius-server auth-port

Function

The **radius-server auth-port** command configures the authentication port for a RADIUS server.

Format

- **radius-server** *name* **auth-port** { *auth-port* | **default** }

Parameters

Parameters	Description	Value
name	Specifies the RADIUS server name.	-
auth-port	Specifies the authentication port number.	The value is an integer in the range from 1 to 65535.
default	Default Value	1812

Default Value

1812

View

AAA configuration view

Usage Guidelines

None

Example

Set the authentication port number of the RADIUS server to 100.

```
switch(config-aaa)#radius-server 111 auth-port 100
switch(config-aaa)#
```

6.8.13 radius-server deadtime

Function

The **radius-server deadtime** command configures the dead time for a RADIUS server.

Format

- **radius-server deadtime** { *deadtime* | **default1** }
- **radius-server** *name* **deadtime** { *deadtime* | **default2** }

Parameters

Parameters	Description	Value
name	Specifies the RADIUS server name.	The value is a character string.
deadtime	Specifies the dead time.	The value is an integer in the range from 3 to 4294967290, in seconds.
default1	Default Value	60 seconds
default2	Default Value	None

Default Value

None

View

AAA configuration view

Usage Guidelines

None

Example

Set the dead time for a RADIUS server.

```
switch(config-aaa)#radius-server deadtime 100
switch(config-aaa)#

switch(config-aaa)#radius-server 111 deadtime 100
switch(config-aaa)#
```

6.8.14 radius-server {ip-address|ip6-address} key

Function

The **radius-server {ip-address|ip6-address} key** command creates a RADIUS server and sets its name, IPv4 or IPv6 address, and shared key.

Format

- **radius-server** *name* **ip-address** *ip4-address* **key** *key*
- **radius-server** *name* **ip6-address** *ip6-address* **key** *key*

Parameters

Parameters	Description	Value
name	Specifies the RADIUS server name.	The value is a character string.
ip4-address	Specifies an IPv4 address.	The value is in the dotted decimal format, for example, A.B.C.D, where A-D are decimal numbers in the range from 0 to 255.
ip6-address	Specifies an IPv6 address	-
key	Indicates the key of the RADIUS server.	-

Default Value

None

View

AAA configuration view

Usage Guidelines

None

Example

Create a radius server and set its name, IPv4 address, and shared key.

```
switch(config-aaa)#radius-server 111 ip-address 1.1.1.1 key 123
switch(config-aaa)#
```

6.8.15 radius-server {ip-address|ip6-address} key auth-port acct-port

Function

The **radius-server {ip-address|ip6-address} key auth-port acc-port** command creates an IPv4 or IPv6 RADIUS server.

Format

- **radius-server** *name* **ip-address** *ipv4-address* **key** *key* **auth-port** { *auth-port* | **default** } **acc-port** { *acc-port* | **default** }
- **radius-server** *name* **ip6-address** *ipv6-address* **key** *key* **auth-port** { *auth-port* | **default** } **acc-port** { *acc-port* | **default** }

Parameters

Parameters	Description	Value
name	Specifies the RADIUS server name.	-
ipv4-address	Specifies an IPv4 address.	The value is in the dotted decimal format, for example, A.B.C.D, where A-D are decimal numbers in the range from 0 to 255.
ipv6-address	Specifies an IPv6 address	-
key	Specifies the shared key of the RADIUS server.	-
auth-port	Specifies the authentication port number.	The value is an integer in the range from 1 to 65535.
default	Indicates the default authentication port number.	1812
acc-port	Specifies the accounting port number.	The value is an integer in the range from 1 to 65535.
default	Indicates the default accounting port number.	1813

Default Value

auth-port: 1812
acc-port: 1813

View

AAA configuration view

Usage Guidelines

None

Example

Create an IPv4 RADIUS server.

```
switch(config-aaa)#radius-server 111 ip-address 1.1.1.1 key 123 auth-port 100 acct-port 100
switch(config-aaa)#
```

6.8.16 radius-server max-retransmit

Function

The **radius-server max-retransmit** command sets the global maximum number of retransmission times for all RADIUS servers or sets the maximum number of retransmission times for specified servers.

Format

- **radius-server max-retransmit** { *max-retransmit* | **default** }
- **radius-server** *name* **max-retransmit** { *max-retransmit* | **default** }

Parameters

Parameters	Description	Value
name	Specifies the RADIUS server name.	The value is a character string.
max-retransmit	Specifies the maximum number of retransmission times.	The value is an integer in the range from 0 to 5.
default	Default Value	The default is 3 in the global configuration view.

Default Value

3

View

AAA configuration view

Usage Guidelines

None

Example

Set the global maximum number of RADIUS server retransmissions.

```
switch(config-aaa)#radius-server 111 max-retransmit 2
switch(config-aaa)#

switch(config-aaa)#radius-server max-retransmit 2
switch(config-aaa)#
```

6.8.17 radius-server retransmit-interval

Function

The **radius-server retransmit-interval** command sets the global maximum number of retransmission times or sets the maximum number of retransmission times for specified servers.

Format

- **radius-server retransmit-interval** { *retransmit-interval* | **default1** }
- **radius-server** *name* **retransmit-interval** { *retransmit-interval* | **default 2** }

Parameters

Parameters	Description	Value
name	Specifies the RADIUS server name.	-
retransmit-interval	Specifies the retransmission interval.	The value is an integer ranging from 1 to 10, in seconds.
default1	Default Value	The default is 2 in the global configuration view.
default2	Default Value	None

Default Value

None

View

AAA configuration view

Usage Guidelines

None

Example

Set the global retransmission interval for all the RADIUS servers.

```
switch(config-aaa)#radius-server retransmit-interval 2
switch(config-aaa)#

switch(config-aaa)# radius-server retransmit-interval 2
switch(config-aaa)#
```

6.8.18 radius-server {src-ip|src-ipv6}

Function

The **radius-server {src-ip|src-ipv6}** command configures the source IP address sending packets to the RADIUS server.
The **no radius-server {src-ip|src-ipv6}** command deletes the source IPv4 or IPv6 address for a RADIUS server.

Format

- **radius-server** *name* **src-ip** *ip-address*
- **no radius-server** *name* **src-ip**
- **radius-server** *name* **src-ipv6** *ipv6-address*
- **no radius-server** *name* **src-ipv6**

Parameters

Parameters	Description	Value
ip-address	Specifies the source IP address of a request packet.	The value is in dotted decimal notation.
ipv6-address	Specifies the source IPv6 address of a request packet.	-
name	Specifies the RADIUS server name.	The value is a character string.

Default Value

None

View

AAA configuration view

Usage Guidelines

None

Example

Configure the source IP address sending packets to a RADIUS server.

```
switch(config-aaa)#radius-server server1 src-ip 1.1.1.1
switch(config-aaa)#
```

6.8.19 reset server statistic

Function

The **reset sever statistic** command clears the statistics ofa specified Tacacs server.

Format

- **reset server** *name* **statistic**

Parameters

Parameters	Description	Value
name	Specifies the name of the Tacacs server.	The value is a character string.

Default Value

None

View

AAA configuration view

Usage Guidelines

None

Example

Clear statistics of a specified Tacacs server.

```
switch(config-aaa)#reset server test1 statistic
switch(config-aaa)#
```

6.8.20 sever-group {radius-server|tacacs-server}

Function

The **server-group {radius-server|tacac-server}** command creates a server group, including defining the server group protocol type and adding a server.

Format

- **sever-group** *name* **radius-server** *server-name*
- **server-group** *name* **tacacs-server** *server-name*

Parameters

Parameters	Description	Value
name	Specifies the server group name.	The value is a character string.
server-name	Specifies the name of a server in the server group.	The value is a character string.
radius-server	Sets the server group protocol type to radius-server.	-
tacacs-server	Sets the server group protocol type to tacacs-server.	

Default Value

None

View

AAA configuration view

Usage Guidelines

None

Example

Create a server group, define its protocol type, and add a server to the group.

```
switch(config-aaa)#server-group aaa radius-server aaa
switch(config-aaa)#
```

6.8.21 show aaa

Function

The **show aaa** command shows AAA information.

Format

- **show aaa**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, and AAA configuration view

Usage Guidelines

None

Example

Show AAA information.

```
switch#show aaa
  Version                              : AAA_VB3.00.00.00
  Account Realtime                     : 300
  Radius-server Retransmit Interval    : 2
  Radius-server Max Retransmit         : 3
  Radius-server Deadtime               : 60
  Tacacs-server Timeout                : 2
  Tacacs-server Deadtime               : 60
switch#
```

6.8.22 show aaa config

Function

The **show aaa config** command displays the global AAA configuration on the switch.

Format

- **show aaa config**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, and AAA configuration view

Usage Guidelines

None

Example

Show AAA configuration file information.

```
switch#show aaa config
Version                                  : AAA_VB3.00.00.00
 aaa
 aaa authentication    enable local method 1
switch#
```

6.8.23 show aaa method

Function

The **show aaa method** command displays information about configured AAA methods.

Format

- **show aaa method**
- **show aaa method** *name*

Parameters

Parameters	Description	Value
name	Specifies an AAA method name	The value is a character string.

Default Value

None

View

Common user view, privileged user view, global configuration view, and AAA configuration view

Usage Guidelines

None

Example

Display information about a configured AAA method.

```
switch#show aaa method
Method Name                          : 1
  Method Apply Type                  : enable
  Method Apply Funtion               : authentication
  Method Local                       : enable
  Method None                        : disable

switch#
```

6.8.24 show aaa server

Function

The **show aaa server** command displays AAA RADIUS server configuration.

Format

- **show aaa server**
- **show aaa server** *name*

Parameters

Parameters	Description	Value
name	Specifies the RADIUS server name.	The value is a character string.

Default Value

None

View

Common user view, privileged user view, global configuration view, and AAA configuration view

Usage Guidelines

None

Example

Displays the configuration of an AAA RADIUS server.

```
switch(config)#show aaa server 111
show aaa server
Server Name                          : 1
  Server IP Address                  : 2.2.2.2
  Server IP Instance                 : public
```

```
  Server Source IP Instance          : public
  Server Key                         : 123
  Server Protocol Type               : radius
  Radius-server Authentication Port  : 1812
  Radius-server Accounting Port      : 1813
  Radius-server Retransmit Interval  : 2
  Radius-server Max Retransmit       : 3
  Radius-server Deadtime             : 60
  Radius-server Source IP Address    : N/A
  Server State                       : active
switch(config)#
```

6.8.25 show aaa server-group

Function

The **show aaa server-group** command displays AAA server group configuration.

Format

- **show aaa server-group**
- **show aaa server-group** *group-name*

Parameters

Parameters	Description	Value
group-name	Specifies the server group name.	The value is a character string.

Default Value

None

View

Common user view, privileged user view, global configuration view, and AAA configuration view

Usage Guidelines

None

Example

Display the configuration of an AAA server group.

```
switch(config)#show aaa server-group aaa
Server-group Name                  : 1
  Server-group Protocol Type       : radius
  Primary Server                   : 1(2.2.2.2:1812:1813)
```

```
Current Active Server                : 1(2.2.2.2:1812:1813)
```

6.8.26 show aaa tacacs-server statistic

Function

The **show aaa tacacs-server statistic** command shows statistics of the Tacacs server.

Format

- **show aaa tacacs-server** *name* **statistic**
- **show aaa tacacs-server statistic**

Parameters

Parameters	Description	Value
name	Specifies the Tacacs server name.	The value is a character string.

Default Value

None

View

Common user view, privileged user view, global configuration view, and AAA configuration view

Usage Guidelines

None

Example

Display statistics about a TACACS server.

```
switch(config)#show aaa tacacs-server ts1 statistic
Server Name                          : 2
  Server IP Instance                 : public
  Server Key                         : 123
  Server Port                        : 49
  Socket Opens                       : 0
  Socket Closes                      : 0
  Socket Errors                      : 0
  Socket Timeouts                    : 0
  Total Packets Sent                 : 0
  Total Packets Recv                 : 0
switch(config)#
```

6.8.27 show radius client

Function

The **show radius client** command displays AAA RADIUS client information.

Format

- **show radius client**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, and AAA configuration view

Usage Guidelines

None

Example

Display AAA RADIUS client information.

```
switch(config)#show radius client
Authentication:
  Server Addresses : 0
  Identifier : FEISU_NAS
  Server Index : 0
    Server Address : 1.1.1.1
    Client Server Port Number : 1812
    Client Round-Trip Time : 0
    Client Access Requests : 0
    Client Access Retransmissions : 0
    Client Access Accepts : 0
    Client Access Rejects : 0
    Client Access Challenges : 0
    Client Malformed Access Responses : 0
    Client Bad Authentications : 0
    Client Pending Requests : 0
    Client Timeouts : 0
    Client Unknown Types : 0
    Client Packets Dropped : 0
```

```
    Client Counter Discontinuity : 0
Account:
  Server Addresses : 0
  Identifier : FEISU_NAS
  Server Index : 0
    Server Address : 1.1.1.1
    Client Server Port Number : 1813
    Client Round-Trip Time : 0
    Client Requests : 0
    Client Retransmissions : 0
    Client Access Accepts : 0
    Client Responses : 0
    Client Malformed Responses : 0
    Client Bad Authentications : 0
    Client Pending Requests : 0
    Client Timeouts : 0
    Client Unknown Types : 0
    Client Packets Dropped : 0
    Client Counter Discontinuity : 0
switch(config)#
```

6.8.28 tacacs-server deadtime

Function

The **tacacs-server deadtime** command configures the Tacacs server dead time.

Format

- **tacacs-server deadtime** { *dead-time* | **default1** }
- **tacacs-server** *name* **deadtime** { *dead-time* | **default2** }

Parameters

Parameters	Description	Value
dead-time	Sets the dead time for a TACACS server.	The value is an integer ranging from 60 to 4294967290. The unit is seconds.
default1	Indicates the default retransmission timeout value.	The default is not configurated.
default2	Indicates the default.	None
name	Specifies the Tacacs server name.	The value is a character string.

Default Value

None

View

AAA configuration view

Usage Guidelines

None

Example

Configure the dead time for a TACACS server.

```
switch(config-aaa)#tacacs-server deadtime 120
switch(config-aaa)#

switch(config-aaa)#tacacs-server feisu deadtime 100
switch(config-aaa)#
```

6.8.29 tacacs-server {ip-address|ip6-address} key

Function

The **tacacs-server {ip-address|ip6-address} key** command creates a TACACS server and sets its name, IPv4 / IPv6 address, and shared key.

Format

- **tacacs-server** *name* **ip-address** *ip-address* **key** *key*
- **tacacs-server** *name* **ip6-address** *ipv6-address* **key** *key*

Parameters

Parameters	Description	Value
name	Specifies the Tacacs server name.	The value is a character string.
ip-address	Specifies an IPv4 address.	The value is in dotted decimal notation.
ipv6-address	Specifies an IPv6 address	-
key	Indicates a shared key.	The length is up to 63 characters.

Default Value

None

View

AAA configuration view

Usage Guidelines

None

Example

Create and configure a Tacacs server, including the server name, IPv4 address, and shared key.

```
switch(config-aaa)#tacacs-server feisu ip-address 10.18.2.36 key feisu
switch(config-aaa)#
```

6.8.30 tacacs-server {ip-address|ipv6-address} key port single-connection

Function

The **tacacs-server {ip-address|ipv6-address} key port single-connection** command creates a Tacacs server, sets its name, IPv4 / IPv6 address, service port, shared key, and enables or disables the single connection function.

Format

- **tacacs-server** *name* **ip-address** *ip-address* **key** *key* **port** { *port-num* | **default** } **single-connection** { **enable** | **disable** }
- **tacacs-server** *name* **ip6-address** *ipv6-address* **key** *key* **port** { *port-num* | **default** } **single-connection** { **enable** | **disable** }

Parameters

Parameters	Description	Value
name	Specifies the Tacacs server name.	The value is a character string.
ip-address	Specifies an IPv4 address.	The value is in dotted decimal notation.
ipv6-address	Specifies an IPv6 address	-
key	Indicates a shared key.	The length is up to 64 characters.
port-num	Specifies the service port.	The value is an integer ranging from 1 to 65535. The default is 49.
enable|disable	Enables or disables the single-connection function.	-

Default Value

Service port 49

View

AAA configuration view

Usage Guidelines

None

Example

Create and configure a Tacacs server.

```
switch(config-aaa)#tacacs-server feisu ip-address 10.18.2.36 key feisu port default single-connection enable
```

```
switch(config-aaa)#
```

6.8.31 tacacs-server port

Function

The **tacacs-server port** command configures the service port of the Tacacs server.

Format

- **tacacs-server** *name* **port** { *port-number* | **default** }

Parameters

Parameters	Description	Value
name	Specifies the Tacacs server name.	The value is a character string.
port-number	Specifies the service port.	The value is an integer ranging from 1 to 65535.
default	Specifies the default service port.	The default is 49.

Default Value

The default is 49.

View

AAA configuration view

Usage Guidelines

None

Example

Configure the service port for a TACACS server.

```
switch(config-aaa)#tacacs-server feisu port 100
switch(config-aaa)#
```

6.8.32 tacacs-server single-connection {enable|disable}

Function

The **tacacs-server single-connection {enable|disable}** command enables or disables the single connection function of a Tacacs server.

Format

- **tacacs-server** *name* **single-connection** { **enable** | **disable** }

Parameters

Parameters	Description	Value
name	Specifies the Tacacs server name.	The value is a character string.
enable|disable	Enables or disables the single-connection function.	-

Default Value

disable

View

AAA configuration view

Usage Guidelines

None

Example

Enable the single-connection function of the TACAS server.

```
switch(config-aaa)#tacacs-server aaa single-connection enable
switch(config-aaa)#
```

6.8.33 tacacs-server {src-ip|src-ipv6}

Function

The **tacacs-server {src-ip|src-ipv6}** command configures the source IP address sending packets to the Tacacs server.

Format

- **tacacs-server** *name* **src-ip** *ip-address*
- **no tacacs-server** *name* **src-ip**
- **tacacs-server** *name* **src-ipv6** *ipv6-address*
- **no tacacs-server** *name* **src-ipv6**

Parameters

Parameters	Description	Value
ip-address	Specifies the source IP address of a request packet.	The value is in dotted decimal notation.
ipv6-address	Specifies the source IPv6 address of a request packet.	-
name	Specifies the Tacacs server name.	The value is a character string.

Default Value

None

View

AAA configuration view

Usage Guidelines

None

Example

Configure the source IP address sending packets to the Tacacs server.

```
switch(config-aaa)#tacacs-server server2 src-ip 2.2.2.2
switch(config-aaa)#
```

6.8.34 tacacs-server timeout

Function

The **tacacs-server timeout** command sets the TACACS server timeout time.

Format

- **tacacs-server** *name* **timeout** { *timeout* | **default1** }
- **tacacs-server timeout** { *timeout* | **default2** }

Parameters

Parameters	Description	Value
name	Specifies the Tacacs server name.	Character string
timeout	Specifies the expiration time	The value is an integer ranging from 1 to 10, in seconds.
default1	Uses the default.	None
default2	Uses the default expiration time	The default is 2s.

Default Value

None

View

AAA configuration view

Usage Guidelines

None

Example

Set the timeout time for a TACACS server.

```
switch(config-aaa)#tacacs-server feisu timeout 10
switch(config-aaa)#
switch(config-aaa)#tacacs-server timeout 5
switch(config-aaa)#
```

6.9 802.1x Configuration Commands

6.9.1 dot1x aaa-account

Function

The **dot1x aaa-account** command binds an AAA accounting method to an interface.
The **no dot1x aaa-account** command unbinds the AAA accounting method from the interface

Format

- **dot1x aaa-account** *account-name*
- **no dot1x aaa-account**

Parameters

Parameters	Description	Value
account-name	Specifies the AAA accounting method name.	The value is a string of 1 to 63 characters.

Default Value

None

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

You can use this command to bind a port with the AAA accounting method name. Before using this command, run the **dot1x interface aaa** command.

Warning: Before using this command, in addition to enable dot1x start globally in the global configuration view (8.10.23 dot1x {start|stop}), you need to enable the interface AAA function globally for the dot1x module in the global configuration view. For details, see 8.10.19 dot1x interface aaa.

Example

Bind interface 10gigaethernet1/02 with AAA accounting method accounttest.

```
switch(config-10ge1/0/2)#dot1x aaa-account accounttest
switch(config-10ge1/0/2)#
```

6.9.2 dot1x aaa-authentication

Function

The **dot1x aaa-authentication** command binds an AAA authentication method to an interface.
The **no dot1x aaa-authentication** command unbinds the AAA authentication method from the interface.

Format

- **dot1x aaa-authentication** *auth-name*
- **no dot1x aaa-authentication**

Parameters

Parameters	Description	Value
auth-name	Specifies the AAA authentication method name	The value is a string of 1 to 63 characters.

Default Value

None

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

You can use this command to bind a port with the AAA authentication method name. Before using this command, run the **dot1x interface aaa** command.

Example

Bind interface 10gigaethernet1/0/1 with AAA authentication method authenticatetest.

```
switch(config-10ge1/0/1)#dot1x aaa-authentication authenticatetest
switch(config-10ge1/0/1)#
```

6.9.3 dot1x authentication auth-method

Function

The **dot1x authentication auth-method** command specifies an authentication method for 802.1x users.

Format

- **dot1x authentication auth-method** { **eap** | **chap** | **pap** }

Parameters

Parameters	Description	Value
eap	Uses Extensible Authentication Protocol (EAP) authentication.	-
chap	Uses Challenge HandshakeAuthentication Protocol (CHAP) authentication.	-
pap	Uses Password Authentication Protocol (PAP) authentication.	-

Default Value

By default, CHAP is adopted for authenticating 802.1x users.

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

Different from the CHAP authentication mode, the EAP authentication mode enables the switch to directly send 802.1x user authentication information to the RADIUS server in EAP packets, rather than converting EAP packets to standard RADIUS packets. You need to enable only the EAP authentication if any of the PEAP, EAP-TLS, EAP-TTLS, or EAP-MD5 authentication modes is adopted.

Warning: When local authentication is adopted, you do not need to configure the EAP authentication mode for authenticating 802.1x users.In the same view, if you repeatedly run the dot1x authentication-method command, the new configuration will overwrite the old configuration.

Example

Set the 802.1x authentication mode on interface 10gigaethernet1/0/1 to EAP.

```
switch(config-10ge1/0/1)#dot1x authentication auth-method eap
switch(config-10ge1/0/1)#
```

6.9.4 dot1x authentication client-timeout

Function

The **dot1x authentication client-timeout** command the timeout period for the response from a supplicant (802.1x client) after the authenticator (switch) sends a Request/MD5-Challenge packet to the supplicant.

Format

- **dot1x authentication client-timeout** { *client-timeout* | **default** }

Parameters

Parameters	Description	Value
client-timeout	Indicates the response timeout duration.	The value is an integer ranging from 1 to 65535, in seconds.

Parameters	Description	Value
default	Specifies the default.	30 seconds

Default Value

By default, the response timeout period is 30 seconds.

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

The 802.1x protocol starts multiple timers to maintain effective, ordered interactions between users (supplicants), access authenticator, and authentication server.
You can use this command to configure the authentication timeout timer of the client. Generally, the default is recommended. In special situations or poor network environment, you can set the Parameters according to actual conditions.
After the authenticator (switch) sends a Request/Challenge packet to a supplicant (client) to request for the MD5 encrypted data, the switch starts the client-timeout timer. If the switch does not receive any response from the client within the timeout period, it retransmits the packet and resets the timer.
The switch does not keep sending the authentication requests. The number of authentication requests is determined by 8.10.7 dot1x authentication max-request.

Example

Set the authentication timeout timer of the client to 50 seconds.

```
switch(config-10ge1/0/1)#dot1x authentication client-timeout 50
switch(config-10ge1/0/1)#
```

6.9.5 dot1x authentication logical-port

Function

The **dot1x authentication logical-port** command sets the logical interface generation mode.

Format

- **dot1x authentication logical-port** { **port-mac** | **port** }

Parameters

Parameters	Description	Value
port-mac	Indicates that a logical port is generated based on the physical port and MAC address.	-
port	Indicates that a logical port is generated only based on the physical port.	-

Default Value

By default, a logical port is generated only based on the port-mac.

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

You can use this command to configure the generation mode of the logical port for 802.1x authentication.

Example

Set the logical interface generation mode to port-mac on interface 10gigaetherne1/0/1.

```
switch(config-10ge1/0/1)#dot1x authentication logical-port port-mac
switch(config-10ge1/0/1)#
```

6.9.6 dot1x authentication max-request

Function

The **dot1x authentication max-request** command sets the maximum number of authentication request retransmissions. This Parameters determines how many times the switch can retransmit authentication requests to a client.

Format

- **dot1x authentication max-request** { *max-request* | **default** }

Parameters

Parameters	Description	Value
max-request	Specifies the maximum retransmission times.	The value is an integer ranging from 1 to 10.
default	Specifies the default.	2

Default Value

By default, the maximum number of retransmission times is 2.

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

If the switch does not receive any response after initially sending the authentication request to the access user, it sends the authentication request again. The maximum number of retransmission times is configured using this command. If the switch still does not receive the response after the maximum number of retransmission times is reached, it does not send the authentication request again.

Example

Set the maximum number of authentication request retransmission to 5 on interface 10gigaethernet 1/0/1.

```
switch(config-10ge1/0/1)#dot1x authentication max-request 5
switch(config-10ge1/0/1)#
```

6.9.7 dot1x authentication max-user

Function

The **dot1x authentication max-user** command sets the maximum number of 802.1x users allowed on an interface.

Format

- **dot1x authentication max-user** *max-user*

Parameters

Parameters	Description	Value
max-user	Specifies the maximum number of users.	The value is an integer ranging from 1 to 256.

Default Value

The default number of users is associated with the switch. It is set to the maximum number of users/maximum number of ports. The maximum number of 802.1x users allowed by the interface is 256.

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

You can use this command to configure the maximum number of 802.1x users allowed on an interface. If the maximum number of users configured for the interface exceeds the maximum number of users supported by the switch, the actual number of access users may be different from the configuration.

Example

Set the maximum number of 802.1x users allowed on an interface on interface 10gigaethernet1/0/1 to 100.

```
switch(config-10ge1/0/1)#dot1x authentication max-user 100
switch(config-10ge1/0/1)#
```

6.9.8 dot1x authentication quiet-period

Function

The **dot1x authentication quiet-period** command sets the quiet period for 802.1x users who fail the authentication on an interface.

Format

- **dot1x authentication quiet-period** { *quiet-period* | **default** }

Parameters

Parameters	Description	Value
quiet-period	Specifies the quiet period for users who fail the authentication.	The value is an integer ranging from 1 to 120, in seconds.
default	Specifies the default.	60 seconds

Default Value

By default, the quiet period for users who fail the authentication is set to 60 seconds.

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

After the quiet timer is enabled, the switch enters the quiet state if the 802.1x user fails the authentication. This can prevent the shock to the system due to frequent authentication. During the quiet period, the switch drops the 802.1x authentication requests and does not handle any 802.1x authentication-related requests.
Generally, the default is recommended. In special situations or poor network environment, you can set the Parameters according to actual conditions.

Example

Set quiet period for 802.1x users who fail the authentication to 80 seconds on interface 10gigaethernet 1/0/1.

```
switch(config-10ge1/0/1)#dot1x authentication quiet-period 80
switch(config-10ge1/0/1)#
```

6.9.9 dot1x authentication reauthenticate-period

Function

The **dot1x authentication reauthenticate-period** command sets the 802.1x re-authentication interval on an interface.

Format

- **dot1x authentication reauthenticate-period** { *reauthenticate-period* | **default** }

Parameters

Parameters	Description	Value
reauthenticate-period	Specifies the re-authentication interval.	The value is an integer ranging from 60 to 7200, in seconds.
default	Specifies the default.	3600 seconds

Default Value

The default 802.1x re-authentication interval is 3600 seconds.

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

You can use this command to set the re-authentication interval.
Generally, the default is recommended. In special situations or poor network environment, you can set the Parameters according to actual conditions.

Example

Set 802.1x re-authentication interval to 1000 seconds on interface 1 0 gigaethernet 1/0/1

```
switch(config-10ge1/0/1)#dot1x authentication reauthenticate-period 1000
switch(config-10ge1/0/1)#
```

6.9.10 dot1x authentication server-timeout

Function

The **dot1x authentication server-timeout** command sets the timeout period for the authentication server on an interface.

Format

- **dot1x authentication server-timeout** { *server-timeout* | **default** }

Parameters

Parameters	Description	Value
server-timeout	Sets the timeout period of the authentication server.	The value is an integer ranging from 1 to 65535, in seconds
default	Specifies the default.	30 seconds

Default Value

By default, the timeout period of the authentication server is 30 seconds.

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

You can use this command to set the authentication server timer. If the authentication server does not respond within the specified period, the switch re-transmits the authentication request.
Generally, the default is recommended. In special situations or poor network environment, you can set the Parameters according to actual conditions.

Example

Set the timeout period of the authentication server to 100 seconds on interface 10gigaethernet 1/0/1.

```
switch(config-10ge1/0/1)#dot1x authentication server-timeout 100
switch(config-10ge1/0/1)#
```

6.9.11dot1x authentication tx-period

Function

The **dot1x authentication tx-period** command the authentication request retransmission interval upon timeout of the response from a client after the switch sends a Request/Identity packet to the client.

Format

- **dot1x authentication tx-period** { *tx-period* | **default** }

Parameters

Parameters	Description	Value
tx-period	Indicates the response timeout duration..	The value is an integer ranging from 1 to 65535, in seconds.
default	Specifies the default.	30 seconds

Default Value

By default, the interval for sending the authentication requests is 30 seconds.

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

You can use this command to enable the 802.1x tx-period timer of the switch.
The switch enables the timer after it sends the unicast Request/Identity request to the client in the case of authentication initiated by the client. If the switch does not receive any response from the client before the timer expires, the switch send the request again.
For a 802.1x client that does not actively initiate authentication, the switch periodically sends the multicast Request/Identity request to the client when enabling a 802.1x port at an interval of tx-period.
Generally, the default is recommended. In special situations or poor network environment, you can set the Parameters according to actual conditions.

Example

On interface 10gigaethernet 1/0/1, set the interval for sending Request/Identity requests after the timer expires to 100 seconds.

```
switch(config-10ge1/0/1)#dot1x authentication tx-period 100
switch(config-10ge1/0/1)#
```

6.9.12 dot1x default aaa-account

Function

The **dot1x default aaa-account** command binds an AAA accounting method name with a 802.1x user
The **no dot1x default aaa-account** command unbinds an AAA accounting method name with a 802.1x user.

Format

- **dot1x default aaa-account** *account-name*
- **no dot1x default aaa-account**

Parameters

Parameters	Description	Value
account-name	Specifies the AAA accounting method name.	The value is a string of 1 to 63 characters.

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to bind/unbind a port with the AAA accounting method name

Example

Bind a port with the AAA accounting method named accounttest.

```
switch(config)#dot1x default aaa-account accounttest
switch(config)#
```

6.9.13 dot1x default aaa-authentication

Function

The **dot1x default aaa-authentication** command binds an AAA authentication method name with a 802.x1 user.
The **no dot1x default aaa-authentication** command unbinds an AAA authentication method name with a 802.x1 user.

Format

- **dot1x default aaa-authentication** *auth-name*
- **no dot1x default aaa-authentication**

Parameters

Parameters	Description	Value
auth-name	Specifies the AAA authentication method name.	The value is a string of 1 to 64 characters.

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to bind/unbind a port with the AAA authentication method name.

Example

Bind a port with the AAA authentication method named authtest.

```
switch(config)#dot1x default aaa-authentication authtest
switch(config)#
```

6.9.14 dot1x default supplicant-support

Function

The **dot1x default supplicant-support** command globally configures the default client type

Format

- **dot1x default supplicant-support** { **normal** | **sep** }

Parameters

Parameters	Description	Value
normal	Specifies the normal mode.	-
sep	Specifies the Symantec mode	-

Default Value

Normal

View

Global configuration view

Usage Guidelines

In normal mode, the client actively sends the start request. In Symantec mode, the switch actively sends a request when the port link is in the Up state.

Example

Globally configure the default client type to sep.

```
switch(config)#dot1x default supplicant-support sep
switch(config)#
```

6.9.15 dot1x default vlan-assignment-mode

Function

The **dot1x default vlan-assignment-mode {integer|string}** command sets the VLAN assignment mode on an interface using 802.1x authentication.

Format

- **dot1x default vlan-assignment-mode** { **integer** | **string** }

Parameters

Parameters	Description	Value
integer	integer type.	-
string	string type	-

Default Value

string

View

Global configuration view

Usage Guidelines

Generally, the authentication dot1x server supports INT or STRING types of VLAN issuing. You can determine the configuration on the device with the command based on the VLAN issuing type of the dot1x authentication server
In string mode, a special server is required to achieve the function.

Example

Set the VLAN type to integer.

```
switch(config)#dot1x start
switch(config)#dot1x default vlan-assignment-mode integer
switch(config)#
```

6.9.16 dot1x {enable|disable}

Function

The **dot1x {enable|disable}** command enables or disables the 802.1x function on an interface

Format

- **dot1x** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the 802.1x function on an interface.	-
disable	Disables the 802.1x function on an interface.	-

Default Value

By default, the 802.1x function is disabled on an interface.

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

Before using this command, you can run the **dot1x {start|stop}** command to enable the global 802.1x function.
Before disabling the 802.1x function at a port, ensure that this port does not serve any online user

Example

Enable the 802.1x function on interface 10gigaethernet 1/0/1.

```
switch(config-10ge1/0/1)#dot1x enable
switch(config-10ge1/0/1)#
```

6.9.17 dot1x guest vlan

Function

The **dot1x guest vlan** command configures a guest VLAN on an interface.
The **no dot1x guest vlan** command deletes the guest VLAN on an interface.

Format

- **dot1x guest vlan** *vlan-id*
- **no dot1x guest vlan**

Parameters

Parameters	Description	Value
vlan-id	Specifies the Guest VLAN.	The value is an integer ranging from 1 to 4094

Default Value

By default, the Guest VLAN is not configured for the interface.

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

You can use this command to configure a guest VLAN on an interface.
After the Guest VLAN is configured, a user who fails the authentication can access the resources in the Guest VLAN only. After the authentication is successful, the user is switched to the original service VLAN. The configuration of the service VLAN and the Guest VLAN must be different.

Warning: The Guest VLAN must be created and cannot be assigned a PVID that is the same as that of the interface.
After the Guest VLAN is configured for an interface, you cannot add this interface to the VLAN again or delete the VLAN.
Different interfaces can be added to different Guest VLANs.
If you run this command repeatedly in the same view, the new configuration will overwrite the old configuration.
Before configuring a Guest VLAN on an interface, set **dot1x authentication max-user** to 1.

Example

Set the Guest VLAN on interface 10gigaethernet 1/0/1 to VLAN 100.

```
switch(config-10ge1/0/1)#dot1x guest vlan 100
switch(config-10ge1/0/1)#
```

6.9.18 dot1x interface aaa

Function

The **dot1x interface aaa** command enables or disables AAA method binding on an interface

Format

- **dot1x interface aaa** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables AAA method name binding with the interface.	-
disable	Disables Enables AAA method name binding with the interface.	-

Default Value

By default, AAA method name binding with the interface is disabled.

View

Global configuration view

Usage Guidelines

You can use this command to determine whether to bind a port with the AAA authentication method name.

Example

Enable AAA method name binding with the interface.

```
switch(config)#dot1x interface aaa enable
switch(config)#
```

6.9.19 dot1x link-mode

Function

The **dot1x link-mode** command sets the working mode of an interface.

Format

- **dot1x link-mode** { **passive** | **active** }

Parameters

Parameters	Description	Value
passive	Indicates that the port works in passive mode.	-
active	Indicates that the port works in active mode.	-

Default Value

By default, an interface works in passive mode.

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

You can use this command to set the working mode of a port, including active and passive..

Example

Configure interface 10gigaethernet 1/0/1 to work in active mode.

```
switch(config-10ge1/0/1)#dot1x link-mode active
switch(config-10ge1/0/1)#
```

6.9.20 dot1x mac-delete-notify

Function

The **dot1x mac-delete-notify** command determines whether to delete a user when configuring the MAC table aging

Format

- **dot1x mac-delete-notify** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the function of deleting a user when configuring the MAC table aging.	-
disable	Disables the function of deleting a user when configuring the MAC table aging	-

Default Value

disable

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

None

Example

Enable the function of deleting a user when configuring the MAC table aging.

```
switch(config-100ge1/0/1)#dot1x mac-delete-notify enable
switch(config-100ge1/0/1)#
```

6.9.21 dot1x reauthenticate

Function

The **dot1x reauthenticate** command enables or disables 802.1x re-authentication on an interface.

Format

- **dot1x reauthenticate** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables re-authentication on an interface.	-
disable	Disables re-authentication on an interface.	-

Default Value

By default, 802.1x re-authentication is disabled on an interface.

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

You can use this command to enable or disable the re-authentication function on an interface. After you run this command, the switch periodically triggers re-authentication according to the re-authentication period. You do not need to manually enter the user name during re-authentication.

Example

Enable 802.1x re-authentication on interface 10gigaethernet1/0/1.

```
switch(config-10ge1/0/1)#dot1x reauthenticate enable
switch(config-10ge1/0/1)#
```

6.9.22 dot1x {start|stop}

Function

The **dot1x {start|stop}** command enables or disables the 802.1x protocol globally.

Format

- **dot1x {start|stop}**

Parameters

Parameters	Description	Value
start	Enables the 802.1x protocol globally.	-
stop	Disables the 802.1x protocol globally.	-

Default Value

By default, the 802.1x protocol is disabled globally

View

Global configuration view

Usage Guidelines

You can use this command to enable or disable the 802.1x protocol globally. This command is a prerequisite command for configuring other 802.1x Parameters. Other configuration takes effect only after the 802.1x protocol is enabled globally.

Example

Enable the 802.1x protocol globally.

```
switch(config)#dot1x start
```

```
switch(config)#
```

6.9.23 dot1x supplicant-support

Function

The **dot1x supplicant-support** command globally configures the default client type.

Format

- **dot1x supplicant-support** { **normal** | **sep** }

Parameters

Parameters	Description	Value
normal	Specifies the normal mode.	-
sep	Specifies the Symantec mode.	-

Default Value

None

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

The default mode is normal. In normal mode, the client actively sends the start request. In Symantec mode, the switch actively sends a request when the port link is in the Up state.

Example

Configure the default client type.

```
switch(config-100ge1/0/1)#dot1x supplicant-support sep
switch(config-100ge1/0/1)#
```

6.9.24 dot1x vlan-assignment-mode

Function

The **dot1x vlan-assignment-mode** command sets the VLAN assignment mode on an interface using 802.1x authentication.

Format

- **dot1x vlan-assignment-mode** { **integer** | **string** }

Parameters

Parameters	Description	Value
integer	integer type.	-
string	String type	-

Default Value

string

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

Generally, the authentication dot1x server supports INT or STRING types of VLAN issuing. You can determine the configuration on the device with the command based on the VLAN issuing type of the dot1x authentication server.
In string mode, a special server is required to achieve the function.

Example

Set the VLAN type to integer on an interface.

```
switch(config)#dot1x start
switch(config)#interface 10gigaethernet 1/0/1
switch(config-10ge1/0/1)#dot1x enable
switch(config-10ge1/0/1)#dot1x vlan-assignment-mode integer
switch(config-10ge1/0/1)#
```

6.9.25 no dot1x authentication user all

Function

The **no dot1x authentication user all** command deletes all 802.1x users.

Format

- **no dot1x authentication user all**

Parameters

None

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to deletes all 802.1x users

Example

Delete all 802.1x users.

```
switch(config)#no dot1x authentication user all
switch(config)#
```

6.9.26 no dot1x interface user all

Function

The **no dot1x interface user all** command deletes all users on an interface.

Format

- **no dot1x interface** { **10gigaethernet** | **100gigaethernet** } *interface-number* **user all**

Parameters

Parameters	Description	Value
{ 10gigaethernet | 100gigaethernet }	Specifies a 10Gigabit Ethernet interface or 100GB Ethernet interface.	-
interface-number	Specifies an Ethernet interface number.	The value is an integer. <1-1>/<0-2>/<1-52>

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to delete all users on an interface.

Example

Delete all users on interface 10gigaethernet 1/0/1.

```
switch(config)#no dot1x interface 10gigaethernet 1/0/1 user all
switch(config)#
```

6.9.27 show dot1x authentication user

Function

The **show dot1x authentication user** command displays user information on interfaces

Format

- **show dot1x authentication user**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet), and interface group configuration view

Usage Guidelines

You can use this command to show interface user information.

Example

Display interface user information.

```
switch#show dot1x authentication user
Max support user:256
 Current user:0
switch#
```

6.9.28 show dot1x config

Function

The **show dot1x config** command shows global dot1x configuration

Format

- **show dot1x config**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet), and interface group configuration view

Usage Guidelines

None

Example

Display global dot1x configuration.

```
switch(config-100ge1/0/1)#show dot1x config
Version                                 :DOT1X_VB3.00.00.00
 dot1x start

 interface 100ge-1/0/1
 dot1x enable
 dot1x authentication max-user 1
 dot1x authentication auth-method eap
 dot1x guest vlan 1
switch(config-100ge1/0/1)#
```

6.9.29 show dot1x interface

Function

The **show dot1x interface** command displays 802.1x information on all interfaces or a specified interface.

Format

- **show dot1x interface**
- **show dot1x interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*

Parameters

Parameters	Description	Value
{ 10gigaethernet | 100gigaethernet }	Specifies a 10Gigabit Ethernet interface or 100GB Ethernet interface.	-
interface-number	Specifies the interface card number or interface number.	The value is an integer. For a fixed interface, the value is <1-1>/<0-2>/<1-52>

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet), and interface group configuration view

Usage Guidelines

If no interface number is specified, this command shows all port information. If an interface number is specified, this command shows information about the specified port.

Example

Display information about interface 10gigaethernet 1/0/1.

```
switch(config)#show dot1x interface 10gigaethernet 1/0/1
dot1x enable
 dot1x authentication max-user :1
 dot1x reauthenticate :disable
 dot1x authentication quiet-period :60
 dot1x authentication reauthenticate-period :3600
 dot1x authentication tx-period :30
 dot1x authentication client-timeout :30
 dot1x authentication max-request :2
 dot1x authentication logical-port :port-mac
 dot1x authentication auth-method :eap
 dot1x link-mode :passive
 dot1x guest vlan    :1
 dot1x supplicant-support :normal
switch(config)#
```

6.9.30 show dot1x statistic

Function

The **show dot1x statistic** command displays dot1x statistics.

Format

- **show dot1x statistic**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet), and interface group configuration view

Usage Guidelines

You can use this command to show the statistics.

Example

Display the statistics.

```
switch(config)#show dot1x statistic
 10ge-1/0/1 dot1x statistic information:
 In Protocol Version Number :1
 In Source MAC Address :0000:0000:0000
 EAPOL Packets statistic:
 Out   Packets    :0        In   Packets      :0
  Out          EAPOL Request/Identity Packets        :0
               EAPOL Request/Challenge Packets       :0
               EAPOL Success Packets                 :0
               EAPOL Failure Packets                 :0
  In           EAPOL Start Packets                   :0
               EAPOL LogOff Packets                  :0
               EAPOL Response/Identity Packets       :0
               EAPOL Response/Challenge Packets      :0
               EAPOL Response/Nak Packets            :0
               EAPOL Invalid Packets                 :0
               EAPOL Length Error Packets            :0
switch(config)#
```

6.9.31 show dot1x statistic {10gigaethernet|100gigaethernet}

Function

The **show dot1x statistic {10gigaethernet|100gigaethernet}** command displays statistics of an interface

Format

- **show dot1x statistic** { **10gigaethernet** | **100gigaethernet** } *interface-number*

Parameters

Parameters	Description	Value
{ 10gigaethernet | 100gigaethernet }	Specifies a 10Gigabit Ethernet interface or 100GB Ethernet interface.	-
interface-number	Specifies the interface card number or interface number.	The value is an integer. For a fixed interface, the value is <1-1>/<0-2>/<1-52>

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet), and interface group configuration view

Usage Guidelines

You can use this command to show the statistics of an interface

Example

Display statistics on interface 10gigaethernet 1/0/1.

```
switch(config)#show dot1x statistic 10gigaethernet 1/0/1
 10ge-1/0/1 dot1x statistic information:
 In Protocol Version Number :1
 In Source MAC Address :0000:0000:0000
 EAPOL Packets statistic:
 Out   Packets    :0        In   Packets      :0
  Out          EAPOL Request/Identity Packets        :0
               EAPOL Request/Challenge Packets       :0
               EAPOL Success Packets                 :0
               EAPOL Failure Packets                 :0
  In           EAPOL Start Packets                   :0
               EAPOL LogOff Packets                  :0
               EAPOL Response/Identity Packets       :0
               EAPOL Response/Challenge Packets      :0
               EAPOL Invalid Packets                 :0
               EAPOL Length Error Packets            :0
switch(config)#
```

6.10 Storm Suppression Configuration Commands

6.10.1storm-suppression log {enable|disable}

Function

The **storm-suppression log {enable|disable}** command enables or disables storm suppression logs.

Format

- **storm-suppression log** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables storm suppression logs.	-

Parameters	Description	Value
disable	Disables storm suppression logs.	-

Default Value

disable

View

Global configuration view

Usage Guidelines

None

Example

Enable storm suppression logs.

```
switch(config)#storm-suppression log enable
switch(config)#
```

6.10.2 storm-suppression trap {enable|disable}

Function

The **storm-suppression trap {enable|disable}** command enables or disables the reporting of storm suppression alarms.

Format

- **storm-suppression trap** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the reporting of storm suppression alarms.	-
disable	Disables the reporting of storm suppression alarms.	-

Default Value

disable

View

Global configuration view

Usage Guidelines

None

Example

Enable the reporting of storm suppression alarms.

```
switch(config)#storm-suppression trap enable
switch(config)#
```

6.10.3 storm-suppression {multicast|broadcast|dlf} min-rate max-rate

Function

The **storm-suppression {multicast|broadcast|dlf} min-rate max-rate** command configures the maximum and minimum percentages or the 64kbps value of storm suppression.
The **no storm-suppression {multicast|broadcast|dlf}** command restores the default for interface storm suppression.

Format

- **storm-suppression** { **multicast** | **broadcast** | **dlf** } **min-rate percent** *percent* **max-rate percent** *percent*
- **storm-suppression** { **multicast** | **broadcast** | **dlf** } **min-rate kbps** *kbps-value*|**mbps** *mbps-value* |**gbps** *gbps-value* **max-rate kbps** *kbps-value*|**mbps** *mbps-value* |**gbps** *gbps-value*
- **no storm-suppression** { **multicast** | **broadcast** | **dlf** }

Parameters

Parameters	Description	Value
multicast	Indicates the multicast messages.	-
broadcast	Indicates the broadcast messages.	-
dlf	Indicates the unicast messages.	-
percent	Indicates the threshold in percentage.	The value is an integer in the range from 1 to 100.
kbps-value	Indicates the kbps threshold.	The value is an integer in the range from 1 to 100000.
mbps-value	Indicates the mbps threshold.	The value is an integer in the range from 1 to 100000.
gbps-value	Indicates the gbps threshold.	The value is an integer in the range from 1 to 100000.

Default Value

None

View

Interface configuration view (Ethernet) and batch interface configuration view

Usage Guidelines

None

Example

Set the maximum and minimum percentages of storm suppression to 10% and 50% respectively.

```
switch(config-100ge1/0/1)#storm-suppression multicast min-rate percent 10 max-rate percent 50
switch(config-100ge1/0/1)#
```

6.10.4 storm-suppression action {block|error-down|none}

Function

The **storm-suppression action {block|error-down|none}** command configures the storm suppression action.

Format

- **storm-suppression action** { **block** | **error-down** | **none** }

Parameters

Parameters	Description	Value
block	Blocks messages.	-
error-down	Disables the interface.	-
none	Indicates no action	-

Default Value

None

View

Interface configuration view (Ethernet) and batch interface configuration view

Usage Guidelines

None

Example

Configure the storm suppression action to "block".

```
switch(config-100ge1/0/1)#storm-suppression action block
switch(config-100ge1/0/1)#
```

6.10.5 storm-suppression interval

Function

The **storm-suppression interval** command configures the detection interval for storm suppression.

Format

- **storm-suppression interval** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	Specifies the detection interval for storm suppression.	The value is an integer ranging from 1 to 108, in seconds.
default	Indicates the default interval.	5 seconds

Default Value

5 seconds

View

Interface configuration view (Ethernet) and batch interface configuration view

Usage Guidelines

None

Example

Configure the detection interval for storm suppression to 10s.

```
switch(config-100ge1/0/1)#storm-suppression interval 10
switch(config-100ge1/0/1)#
```

6.10.6 show storm-suppression interface

Function

The **show storm-suppression interface** command displays the Ethernet interface information of storm suppression.

Format

- **show storm-suppression interface**
- **show storm-suppression interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer string in the range of <1-1>/<0-2>/<1-52>.

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Display the Ethernet interface information of storm suppression.

```
switch(config)#show storm-suppression interface 10gigaethernet 1/0/1
Interface Type      mode      Status   Min-rate   Max-rate   Action      Interval
10ge-1/0/1   multicast    pps          disable 0              0             none         0
10ge-1/0/1   broadcast    pps          disable 0              0             none         0
10ge-1/0/1    dlf             pps          disable 0              0             none         0
switch(config)#
```

6.10.7 show storm-suppression config

Function

The **show storm-suppression config** command displays the configuration of storm suppression.

Format

- **show storm-suppression config**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Display the configuration of storm suppression.

```
switch(config)#show storm-suppression config
storm-suppression trap enable
interface 10ge-1/0/1
 storm-suppression interval 1
```

```
 storm-suppression multicast min-rate 100 max-rate 1000
switch(config)#
```

7. Reliability Commands

7.1 Overview

This chapter introduces the equipment reliability configuration commands of the N-series switch.

7.2 MSTP Configuration Commands

7.2.1 no stp instance

Function

The **no stp instance** command is used to delete a spanning tree instance.

Format

- **no stp instance** *instance-id*

Parameters

Parameters	Description	Value
instance-id	Specifies the ID of a spanning tree instance.	The value is an integer in the range from 1 to 63.

Default Value

None

View

STP configuration view

Usage Guidelines

You can use this command to delete a spanning tree instance.

Example

Delete spanning tree instance 36.

```
switch(config-stp)#no stp instance 36
switch(config-stp)#
```

7.2.2 show stp

Function

The **show stp** command is used to display the configuration of the STP protocol on the switch.

Format

- **show stp**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, STP configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

You can use this command to check the configuration of the STP protocol running on the switch.

Example

Check the configuration of the STP protocol running on the switch.

```
switch#show stp
Version                                : MSTP_VB3.70.00.00
Oper Configuration
Stp Mode                               : mstp
Stp Trap                               : disable
Stp BPDU-guard                         : disable
Stp TC-protection                      : disable
Stp TC-protection Threshold            : 2
Bridge Times                           : Hello 2s MaxAge 20s FwDly 15s MaxHop 20 Timer Factor 6
Format Selector                        : 0
Revision Level                         : 0
Stp Config Name                        : region
Stp TC-flush-arp                       : disable
Stp Migration-time                     : 3
Stp Pathcost-standard                  : dot1t
Stp Tc-hold-off                        : 10
Stp Transmit-limit                     : 6 packets/s
Stp Link-detection                     : enable
Stp Edge-default                       : disable
Stp Instance max Number                : 64
Stp Instance used Number               : 1
Stp Interface max Number               : 36
Stp Interface used Number              : 1
Stp Interface Instance max Number      : 2304
Stp Interface Instance used Number     : 1
```

```
Instance Priority Vlans Mapped
0        32768    1-4094

switch#
```

7.2.3 show stp brief

Function

The **show stp brief** command is used to display the status of the interface configured with the STP.

Format

- **show stp brief**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, STP configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

None

Example

View the status of the interface configured with the STP.

```
switch#show stp brief
 MSTID Port          Role          STP State     Protection    Region
 0     10ge-1/0/1    designated    forward       N/A           same
 0     10ge-1/0/2    designated    forward       N/A           same
switch#
```

7.2.4 show stp config

Function

The **show stp config** command is used to display the configuration file of the STP protocol running on the switch.

Format

- **show stp config**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, STP configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

You can use this command to check the configuration file of the spanning tree protocol running on the switch.

Example

Display the configuration file of the STP protocol running on the switch.

```
switch#show stp config
  Version: MSTP_VB3.01.00.00
  stp
  stp bpdu-guard enable
  interface 10gigaethernet 1/0/1
  stp root-guard enable

switch#
```

7.2.5 show stp information

Function

The **show stp information** command is used to display information about the STP protocol running on the switch.

Format

- **show stp information**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, STP configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

You can use this command to check information about the STP protocol running on the switch, including the CIST and MSTI.

Example

Check information about the STP protocol running on the switch.

```
switch#show stp information
 CIST Bridge          : 32768.0005-67fc-c1cb
 Bridge Times         : Hello 2s MaxAge 20s FwDly 15s RemainingHops 20
 CIST Root/ERPC       : 32768.0005-67fc-c1cb/ 0
 CIST RegRoot/IRPC    : 32768.0005-67fc-c1cb/ 0
 Number of TC         : 0
 Last TC occurred     : N/A

switch#
```

7.2.6 show stp instance interface

Function

The **show stp instance interface** command is used to display the spanning tree instance configuration at all interfaces.
The **show stp instance interface {10gigaethernet|100gigaethernet|eth-trunk}** command is used to display the STP instance configuration at a specified interface.

Format

- **show stp instance** *instance-id* **interface**
- **show stp instance** *instance-id* **interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **show stp instance** *instance-id* **interface eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
instance-id	Specifies an MSTI number.	The value is an integer in the range from 0 to 63.
interface-number	Specifies an Ethernet interface number.	The value is an integer string in the range of <1-1>/<0-2>/<1-52>.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 124.

Default Value

None

View

Common user view, privileged user view, global configuration view, STP configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

You can use this command to check the STP information at all interfaces or a specified interface.

Example

Check the information about spanning tree instance 0 on interface 10gigaethernet 1/0/1.

```
switch#show stp instance 0 interface 10gigaethernet 1/0/1
 --------[CIST Info]--------
 CIST Bridge                 : 32768.0005-67fc-c1cb
 Bridge Times                : Hello 2s MaxAge 20s FwDly 15s RemainingHops 20
 CIST Root/ERPC              : 32768.0005-67fc-c1cb / 0
 CIST RegRoot/IRPC           : 32768.0005-67fc-c1cb / 0
 Number of TC                : 0
 Last TC occurred            : N/A

 --------[PORT Info]--------
 Description                 : 10ge-1/0/1
 Port Role                   : disable
 STP State                   : discarding
 Priority                    : 128
 Port Cost(Dot1t)            : config=auto / active=200000000
 Desg. Bridge/Port           : 32768.0005-67fc-c1cb    / 128.1089
 TC or TCN TX                : 0
 TC or TCN RX                : 0
 Last forwarding time        : 2019/10/17    09:07:03
 Port Edged                  : config=disable / active=disable
 Point-to-point              : config=auto / active=false
 TCN RX                      : 0
 Config RX                   : 0
 RSTP RX                     : 0
 MSTP RX                     : 0
 TCN TX                      : 0
 Config TX                   : 0
 RSTP TX                     : 0
 MSTP TX                     : 0
 BPDU Filter                 : disable
 Protection Type             : root
switch#
```

Check the information about spanning tree instance 0 on all the interfaces.

```
switch#show stp instance 0 interface
MSTID Port                Role              STP State         Protection
```

7.2.7 show stp interface

Function

The **show stp interface** command is used to display the STP configuration at all interfaces.

Format

- **show stp interface**

Parameters

None

Default Value

Disable

View

Common user view, privileged user view, global configuration view, STP configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

You can use this command to check the STP configuration at all interfaces.

Example

Check the STP configuration at all interfaces.

```
switch#show stp interface
  MSTID Port        Role              STP State        Protection       Region
  0     10ge-1/0/1  disable           discarding       root             N/A
  0     10ge-1/0/2  disable           discarding       N/A              N/A
  0     10ge-1/0/3   disable          discarding       N/A              N/A
  more
  0      eth-trunk-1 disable          discarding       N/A              N/A
switch#
```

7.2.8 show stp interface {10gigaethernet|100gigaethernet|eth-trunk}

Function

The **show stp interface {10gigaethernet|100gigaethernet|eth-trunk}** command is used to display the STP configuration at a specified interface.

Format

- **show stp interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **show stp interface eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer string in the range of <1-1>/<0-2>/<1-52>.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 124.

Default Value

None

View

Common user view, privileged user view, global configuration view, STP configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

You can use this command to check the STP configuration at an interface.

Example

Check the STP configuration at interface 100gigaethernet 1/0/1.

```
switch#show stp interface 100gigaethernet 1/0/1
    --------[CIST Info]--------
    CIST Bridge                 : 32768.6821-5ffb-0854
    Bridge Times                : Hello 2s MaxAge 20s FwDly 15s RemainingHops 20
    CIST Root/ERPC              : 32768.6821-5ffb-0854 / 0
    CIST RegRoot/IRPC           : 32768.6821-5ffb-0854 / 0

    --------[PORT Info instance 0]--------
    Description                 : 100ge1/0/1
    Port Role                   : disable
    STP State                   : discarding
    Priority                    : 128
    Port Cost(Dot1t)            : config=auto / active=200000000
    Desg. Bridge/Port           : 32768.6821-5ffb-0854    / 128.1089
    TC or TCN TX                : 0
    TC or TCN RX                : 0
    Last forwarding time        : 2000/01/01    00:00:20
    Port Edged                  : config=disable / active=disable
    Point-to-point              : config=auto / active=false
    TCN RX                      : 0
    Config RX                   : 0
```

```
    RSTP RX                    : 0
    MSTP RX                    : 0
    TCN TX                     : 0
    Config TX                  : 0
    RSTP TX                    : 0
    MSTP TX                    : 0
    BPDU Filter                : disable
    Protection Type            : N/A
switch#
```

7.2.9 show stp tc-bpdu statistic

Function

The command is used to display the count of transmitted and received TC / TCN packets.

Format

- **show stp tc-bpdu statistic**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, STP configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

You can use this command to confirm which ports transmit or receive abnormal TC / TCN packets and whether a network failure exists. The port information helps identify the source of faults.

Example

Check the count of transmitted and received TC/TCN packets.

```
switch#show stp tc-bpdu statistic
  ------------------------- STP TC/TCN information -------------------------
  MSTID    Port                TC(Send/Receive)   TCN(Send/Receive)
  0        100ge-1/0/1           0/0                0/0
  0        100ge-1/0/2           0/0                0/0
  0        100ge-1/0/3           0/0                0/0
  0        100ge-1/0/4           0/0                0/0
  0        eth-trunk-1           0/0                0/0
```

```
switch#
```

7.2.10 show stp topology-change

Function

The **show stp topology-change** command is used to display statistics of topology changes.

Format

- **show stp topology-change**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, STP configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

In a layer-2 network where the MSTP is running, a device will clear ARP entries and MAC entries after receiving packets indicating topology changes. If a device receives too many such packets, frequent clearing of ARP entries and MAC entries will cause high CPU usage and bring about unstable network traffic.
You can use this command to check statistics of MSTP / VBST topology changes. If the device's topology changes frequently, it is sure that the network is flapping.

Example

Check statistics of topology changes.

```
switch#show stp topology-change
  CIST topology change information
    Number of topology changes                  :0
    Time since last topology change             :0 weeks 0 days 0 hours 29 minutes 33 seconds
    Topology change last received from          :0005-67fc-c1cb
    Number of generated topologychange traps    :0
    Number of suppressed topologychange traps   :0

switch#
```

7.2.11stp

Function

The **stp** command is used to display the STP configuration view.

Format

- **stp**

Parameters

None

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to switch to the STP configuration view from the global configuration view. Then you can configure STP Parameters there.

Example

Switch to the STP configuration view from the global configuration view.

```
switch(config)#stp
switch(config-stp)#
```

7.2.12 stp bpdu-filter

Function

The **stp bpdu-filter** command is used to enable or disable the BPDU filter.

Format

- **stp bpdu-filter** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the BPDU filter.	-
disable	Disables the BPDU filter.	-

Default Value

disable

View

Interface configuration view (Ethernet and trunk) and interface group configuration view

Usage Guidelines

After the BPDU filter is enabled for the spanning tree at an interface, the interface will not send and receive the spanning tree packets. This forms a network loop. Unless otherwise specified, this function is not required.

Example

Enable the BPDU filter.

```
switch(config-100ge1/0/1)#stp bpdu-filter enable
switch(config-100ge1/0/1)#
```

7.2.13 stp bpdu-guard

Function

The **stp bpdu-guard** command is used to enable or disable the BPDU guard.

Format

- **stp bpdu-guard** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the BPDU guard.	-
disable	Disables the BPDU guard.	-

Default Value

By default, the BPDU guard is disabled.

View

STP configuration view

Usage Guidelines

Generally, an access port is directly connected to a user terminal (such as a PC) or file server. You can set access ports as edge ports to achieve fast migration of these ports. In normal situations, an edge port does not receive STP configuration messages (BPDU packets). However, if someone forges configuration messages to maliciously attack the switch, the system automatically sets an edge port as a non-edge port upon receiving the configuration message. This will cause re-calculation of the spanning tree and result in network topology flapping. The BPDU guard can prevent this problem.

Example

Enable the BPDU guard.

```
switch(config-stp)#stp bpdu-guard enable
switch(config-stp)#
```

7.2.14 stp config-name

Function

The **stp config-name** command is used to set the spanning tree domain name.
The **no stp config-name** command is used to clear the spanning tree domain name.

Format

- **stp config-name** *string*
- **no stp config-name**

Parameters

Parameters	Description	Value
string	Specifies the spanning tree domain name.	The value is a string of characters without spaces.

Default Value

The default spanning tree domain name is F-engine.

View

STP configuration view

Usage Guidelines

The MSTP domain name, MSTP domain, VLAN mapping table, and MSTP revision level determine the domain of a switch together.

Example

Set the spanning tree domain name to test.

```
switch(config-stp)#stp config-name test
switch(config-stp)#
```

7.2.15 stp {enable|disable}

Function

The **stp {enable|disable}** command is used to enable or disable STP at an interface.

Format

- **stp** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the STP at an interface.	-

Parameters	Description	Value
disable	Disables the STP at an interface.	-

Default Value

By default, the STP is enable at an interface.

View

Interface configuration view (Ethernet and trunk) and interface group configuration view

Usage Guidelines

None

Example

Enable the STP at interface 10gigaethernet 1/0/1.

```
switch(config-10ge1/0/1)#stp enable
switch(config-10ge1/0/1)#
```

7.2.16 stp edge-port

Function

The **stp edge-port** command is used to enable or disable an edge port.

Format

- **stp edge-port** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables an edge port.	-
disable	Disables an edge port.	-

Default Value

By default, the edge port is disabled.

View

Interface configuration view (Ethernet and trunk) and interface group configuration view

Usage Guidelines

An edge port can directly enter the forwarding state without any delay. Generally, the port that is directly connected to a non-switching device such as a user terminal or a server is configured as an edge port.

Example

Set interface 10gigaethernet 1/0/1 as an edge port.

```
switch(config-10ge1/0/1)#stp edge-port enable
switch(config-10ge1/0/1)#
```

7.2.17 stp edge-default

Function

The **stp edge-default** command is used to enable or disable all ports of a switch as edge ports.

Format

- **stp edge-default** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables all ports of a switch as edge ports.	-
disable	Disables all ports of a switch as edge ports.	-

Default Value

By default, all ports of a switch are non-edge ports.

View

STP configuration view

Usage Guidelines

In a layer-2 network where the STP is running, ports connected to terminals do not take part in spanning tree calculation. If they do, the speed of network topology convergence will be affected. If states of these ports change, network flapping may happen and cause user traffic interruption. You can use this command to enable the current port as an edge port so that it will not take part in spanning tree calculation any more. This helps speed up convergence of the network topology and makes the network stabler.

Example

Enable all ports of a switch as edge ports.

```
switch(config-stp)#stp edge-default enable
switch(config-stp)#
```

7.2.18 stp forward-delay

Function

The **stp forward-delay** command is used to set the STP forwarding delay.

Format

- **stp forward-delay** { *forward-delay* | **default** }

Parameters

Parameters	Description	Value
forward-delay	Specifies the STP forwarding delay.	The value is an integer in the range from 4 to 30 (unit: s).
default	Indicates the default.	15 seconds

Default Value

The default STP forwarding delay is 15 seconds.

View

STP configuration view

Usage Guidelines

When the topology changes, the new configuration message spreads across the network after a period of time. This delay is called forwarding delay.
Generally, the default forwarding delay is used.

Example

Set the STP forwarding delay to 10 seconds.

```
switch(config-stp)#stp forward-delay 10
switch(config-stp)#
```

7.2.19 stp hello-time

Function

The **stp hello-time** command is used to set the interval for sending Hello packets.

Format

- **stp hello-time** { *hello-interval* | **default** }

Parameters

Parameters	Description	Value
hello-interval	Specifies the interval for sending STP Hello packets.	The value is an integer in the range from 1 to 10 (unit: s).
default	Specifies the default interval.	2 seconds

Default Value

By default, the interval for sending STP Hello packets is 2 seconds.

View

STP configuration view

Usage Guidelines

The switch sends BPDU packets based on the Hello Time to maintain the stability of the spanning tree.
The Hello Time, Forward Delay, and Max Age must satisfy the following relations:

- 2 × (Forward Delay - 1.0 second) ≥ Max Age
- Max Age ≥ 2 x (Hello Time + 1.0 second)

The MSTP on the entire network can work effectively only if the preceding relations are satisfied. Otherwise, network flapping frequently occurs.
Generally, the default s of these Parameters are recommended.

Example

Set the interval for sending STP Hello packets to 3 seconds.

```
switch(config-stp)#stp hello-time 3
switch(config-stp)#
```

7.2.20 stp instance path-cost

Function

The **stp instance path-cost** command is used to configure the management path cost of the current port in a specified MST instance (MSTI).

Format

- **stp instance** *instance-id* **path-cost** { *path-cost* | **default** }

Parameters

Parameters	Description	Value
instance-id	Specifies the ID of a spanning tree instance.	The value is an integer in the range from 1 to 63.
path-cost	Specifies the port cost.	The value is an integer in the range from 1 to 200000.
default	Indicates the default.	The value is auto-negotiated based on port rate.

Default Value

By default, the instance management path cost is 0. The port path cost is automatically calculated based on port rate.

View

Interface configuration view (Ethernet and trunk) and interface group configuration view

Usage Guidelines

The port path cost in a specified MST instance is a major Parameters for spanning tree calculation. You can configure different path costs for the same interface in different MSTI instances to enable the switch to forward traffic of different VLANs along different physical links, achieving load balancing among VLANs.

Example

Set the port cost of interface 10gigaethernet 1/0/1 in instance 63 to 1000.

```
switch(config-10ge1/0/1)#stp instance 63 path-cost 1000
switch(config-10ge1/0/1)#
```

7.2.21 stp instance priority (in the STP Configuration View)

Function

The **stp instance priority** command is used to configure the MSTI priority of a switch.

Format

- **stp instance** *instance-id* **priority** { *priority* | **default** }

Parameters

Parameters	Description	Value
instance-id	Specifies the ID of a spanning tree instance.	The value is an integer in the range from 1 to 63.
priority	Specifies the switch priority. The smaller the value is, the higher the priority is.	The value is an integer in the range from 0 to 61440. The step is 4096. That is, you can configure 16 priority values such as 0, 4096, and 8192.
default	Indicates the default.	32768

Default Value

The default priority value is 32768.

View

STP configuration view

Usage Guidelines

The priority configured using this command is a major element for spanning tree calculation. You can configure different priority values for each switch in different MSTI instances.
The step is 4096. If the priority value is not configured based on this step, the system prompts the following information: %Failed. Bridge Priority must be in increments of 4096.

%Allowed values are:
0 4096 8192 12288 16384 20480 24576 28672
32768 36864 40960 45056 49152 53248 57344 61440

Example

Set the priority value of the switch in instance 25 to 4096.

```
switch(config-stp)#stp instance 25 priority 4096
switch(config-stp)#
```

7.2.22 stp instance priority (interface configuration view)

Function

The **stp instance priority** command is used to configure the MSTI priority of the current interface.

Format

- **stp instance** *instance-id* **priority** { *priority* | **default** }

Parameters

Parameters	Description	Value
instance-id	Specifies the ID of a spanning tree instance.	The value is an integer in the range from 1 to 63.
priority	Specifies the interface priority.	The value is an integer in the range from 0 to 240, with a step of 16.
default	Indicates the default.	128

Default Value

By default, the priority of the port matching the spanning tree instance is 128.

View

Interface configuration view (Ethernet and trunk) and interface group configuration view

Usage Guidelines

The interface priority is the basis for role selection of an interface in the specified MSTI instance. You can configure different priority values for the same interface in different MSTI instances, achieving load balancing among VLANs.

Example

Set the priority of interface 10gigaethernet 1/0/1 matching the spanning tree instance to 16.

```
switch(config-10ge1/0/1)#stp instance 1 priority 16
switch(config-10ge1/0/1)#
```

7.2.23 stp instance vlan

Function

The **stp instance vlan** command is used to map a specified VLAN to a specified spanning tree instance.
The **no stp instance vlan** command is used to delete the mapping between a specified VLAN and a spanning tree instance.

Format

- **stp instance** *instance-id* **vlan** *vlan-list*
- **no stp instance** *instance-id* **vlan** *vlan-list*

Parameters

Parameters	Description	Value
vlan-list	Specifies a list of VLANs.	The value is an integer in the range from 1 to 4094.

Default Value

By default, all VLANs are mapped to a CIST (MSTI0).

View

STP configuration view

Usage Guidelines

You can use this command to set the mapping between an MSTI and a VLAN.
MSTP divides a switched network into multiple regions, each containing multiple spanning trees that are independent of one another. Each spanning tree is referred to as a multiple spanning tree instance (MSTI), and each region is referred to as a multiple spanning tree region (MST region).
Two switches are in one MST region if they have identical configurations for the following Parameters:

- MST region name
- MSTI-to-VLAN mapping relationship
- MST region revision level

Example

Map VLAN 16 to STP instance 1.

```
switch(config-stp)#stp instance 1 vlan 16
switch(config-stp)#
```

7.3 stp link-detection

Function

The **stp link-detection** command is used to enable or disable the point-to-point link detection.

Format

- **stp link-detection** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the point-to-point link detection of the spanning tree.	-
disable	Disables the point-to-point link detection of the spanning tree.	-

Default Value

By default, the point-to-point link detection of the spanning tree is enabled.

View

STP configuration view

Usage Guidelines

Most links between switches on a network are connected in point-to-point mode.

Example

Disable the point-to-point link detection of the spanning tree.

```
switch(config-stp)#stp link-detection disable
switch(config-stp)#
```

7.3.1 stp loop-guard

Function

The **stp loop-guard** command is used to enable or disable the spanning tree loop guard.

Format

- **stp loop-guard** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the spanning tree loop guard.	-
disable	Disables the spanning tree loop guard.	-

Default Value

disable

View

Interface configuration view (Ethernet and trunk) and interface group configuration view

Usage Guidelines

None

Example

Enable the loop guard.

```
switch(config-100ge1/0/1)#stp loop-guard enable
switch(config-100ge1/0/1)#
```

7.3.2 stp max-age

Function

The **stp max-age** command is used to set the maximum aging time of the spanning tree.

Format

- **stp max-age** { *max-age* | **default** }

Parameters

Parameters	Description	Value
max-age	Specifies the maximum aging time of the spanning tree.	The value is an integer in the range from 6 to 40 (unit: s).
default	Specifies the default maximum aging time.	20 seconds

Default Value

The default maximum aging time of the spanning tree is 20 seconds.

View

STP configuration view

Usage Guidelines

If a port does not receive any configuration message within a specified period of time, the maximum aging timer is triggered. If its lifetime reaches the maximum aging time, the bridge considers that the link connected to the port is faulty and performs fault identification.
Generally, the default forwarding delay is used. Ultra-long maximum aging time results in the failure of identifying link faults in a timely manner. Ultra-short maximum aging time makes a switch incorrectly identify a link fault and perform spanning tree re-calculation frequently.

Example

Set the maximum aging time of the spanning tree to 10 seconds.

```
switch(config-stp)#stp max-age 10
switch(config-stp)#
```

7.3.3 stp max-hop

Function

The **stp max-hop** command is used to set the maximum hop count of a spanning tree in the MST region.

Format

- **stp max-hop** { *max-hop* | **default** }

Parameters

Parameters	Description	Value
max-hop	Specifies the maximum hop count of a spanning tree.	The value is an integer in the range from 4 to 30.
default	Specifies the default maximum hop count.	20

Default Value

The default maximum hop count of the spanning tree is 20.

View

STP configuration view

Usage Guidelines

You can use this command to set the maximum hop count of a spanning tree in the MST region, limiting the network scale.

Example

Set the maximum hop count of a spanning tree to 10.

```
switch(config-stp)#stp max-hop 10
switch(config-stp)#
```

7.3.4 stp mcheck

Function

The **stp mcheck** command is used to configure the current interface to perform the mode check.

Format

- **stp mcheck**

Parameters

None

Default Value

None

View

Interface configuration view (Ethernet and trunk) and interface group configuration view

Usage Guidelines

A device working in RSTP / MSTP mode can automatically migrate to the STP-compatible mode. However, a device working in the STP-compatible mode cannot automatically migrate to the RSTP / MSTP mode. In this case, you must perform a mode check to forcibly trigger the migration. If an MSTP (or RSTP) device is connected to an STP device on the switching network, its port automatically migrates to the STP-compatible mode. If the STP device is removed, the port cannot automatically migrate to the MSTP (or RSTP) mode, and still works in the STP-compatible mode. In this situation, you can perform a mode check to forcibly trigger the port to migrate to the MSTP (or RSTP) mode.

Example

Configure interface 10gigaethernet 1/0/1 to perform the mode check.

```
switch(config-10ge1/0/1)#stp mcheck
switch(config-10ge1/0/1)#
```

7.3.5 stp migration-time

Function

The **stp migration-time** command is used to set the STP conversion interval.

Format

- **stp migration-time** { *migration-time* | **default** }

Parameters

Parameters	Description	Value
migration-time	Specifies the STP conversion interval.	The value is an integer in the range from 1 to 10 (unit: s).
default	Indicates the default.	3 seconds

Default Value

The default STP conversion interval is 3 seconds.

View

STP configuration view

Usage Guidelines

You can use this command to configure the STP conversion interval. This Parameters is applicable to the port protocol migration state machine. The switch switch allows other RSTP bridges in its VLAN to synchronize the port state before its port receives the BPDU packet and changes the Tx BPDU packet type.

Example

Set the STP conversion interval to 6 seconds.

```
switch(config-stp)#stp migration-time 6
switch(config-stp)#
```

7.3.6 stp mode

Function

The **stp mode** command is used to configure the STP working mode of a switch.

Format

- **stp mode** { **mstp** | **stp** | **rstp** | **default** }

Parameters

Parameters	Description	Value
stp	Indicates the STP mode.	-
rstp	Indicates the RSTP mode.	-
mstp	Indicates the MSTP mode.	-
default	Indicates the default.	mstp

Default Value

The default working mode of the STP is MSTP.

View

STP configuration view

Usage Guidelines

In the STP-compatible mode, each port of the switch sends STP BPDU packets.
In the RSTP mode, each port of the switch sends RSTP BPDU packets. Upon discovering that the switch is connected to an STP device, the port automatically migrates to the STP-compatible mode.
In the MSTP mode, each port of the switch sends MSTP BPDU packets. Upon discovering that the switch is connected to an STP device, the port automatically migrates to the STP-compatible mode.

Example

Set the STP working mode to RSTP.

```
switch(config-stp)#stp mode rstp
switch(config-stp)#
```

7.3.7 stp path-cost

Function

The **stp path-cost** command is used to set the management path cost of an interface in instance 0.

Format

- **stp path-cost** { *cost* | **default** }

Parameters

Parameters	Description	Value
cost	Specifies the path cost of an interface.	The value is an integer in the range from 1 to 200000.
default	Indicates the default.	The value is auto-negotiated based on port rate.

Default Value

By default, the management path cost is 0. The path cost is automatically calculated based on port rate.

View

Interface configuration view (Ethernet and trunk) and interface group configuration view

Usage Guidelines

You can use this command to set the management path cost of an interface.

Example

Set the management path cost of interface 10gigaethernet 1/0/1 in instance 0 to 10000.

```
switch(config-10ge1/0/1)#stp path-cost 10000
switch(config-10ge1/0/1)#
```

7.3.8 stp pathcost-standard

Function

The **stp pathcost-standard** command is used to set the standard for calculating the STP interface path cost.

Format

- **stp pathcost-standard** { **dot1t** | **dot1d-1998** }

Parameters

Parameters	Description	Value
{ dot1t | dot1d-1998 }	Specifies the standard for calculating the STP port path cost. The item dot1t indicates the IEEE 802.1t standard, dot1d-1998 the IEEE 802.1D standard released in 1998.	-

Default Value

By default, the standard used to calculate the STP port path cost is **dot1t**.

View

STP configuration view

Usage Guidelines

Generally, interfaces on the same network should use the same calculation method.

Example

Set the standard for calculating the path cost to dot1d-1998.

```
switch(config-stp)#stp pathcost-standard dot1d-1998
switch(config-stp)#
```

7.3.9 stp point-to-point

Function

The **stp point-to-point** command is used to configure point-to-point management at an interface.

Format

- **stp point-to-point** { **force-true** | **force-false** | **auto** }

Parameters

Parameters	Description	Value
force-true	Indicates the point-to-point management state.	-
force-false	Indicates the non-point-to-point management state.	-

Default Value

By default, the interface is in the point-to-point management state.

View

Interface configuration view (Ethernet and trunk) and interface group configuration view

Usage Guidelines

The RSTP and MSTP fast negotiation mechanism is valid only on point-to-point links.

Example

Set interface 10gigaethernet 1/0/1 to the non-point-to-point management state.

```
switch(config-10ge1/0/1)#stp point-to-point force-false
switch(config-10ge1/0/1)#
```

7.3.10 stp priority (STP configuration view)

Function

The **stp priority** command is used to set the priority of CIST instance 0.

Format

- **stp priority** { *priority* | **default** }

Parameters

Parameters	Description	Value
priority	Specifies the switch priority. The smaller the value is, the higher the priority is.	The value is an integer in the range from 0 to 61440. The step is 4096. That is, you can configure 16 priority values such as 0, 4096, and 8192.
default	Indicates the default.	32768

Default Value

The default priority of the CIST instance is 32768.

View

STP configuration view

Usage Guidelines

The step is 4096. If the priority value is not configured based on this step, the system prompts the following information:
%Failed. Bridge Priority must be in increments of 4096.
%Allowed values are:
0 4096 8192 12288 16384 20480 24576 28672
32768 36864 40960 45056 49152 53248 57344 61440

Example

Set the priority of CIST instance 0 to 8192.

```
switch(config-stp)#stp priority 8192
switch(config-stp)#
```

7.3.11stp priority (interface configuration view)

Function

The **stp priority** command is used to set the priority of an interface.

Format

- **stp priority** { *priority* | **default** }

Parameters

Parameters	Description	Value
priority	Specifies the interface priority.	The value is an integer in the range from 0 to 240, with a step of 16.
default	Indicates the default.	128

Default Value

The default priority of an STP interface is 128.

View

Interface configuration view (Ethernet and trunk) and interface group configuration view

Usage Guidelines

You can use this command to set interface priorities for role selection.

Example

Set the priority of interface 10gigaethernet 1/0/1 to 240.

```
switch(config-10ge1/0/1)#stp priority 240
switch(config-10ge1/0/1)#
```

7.3.12 stp reset statistic

Function

The **stp reset statistic** command is used to reset STP statistics.

Format

- **stp reset statistic**

Parameters

None

Default Value

None

View

Interface configuration view (Ethernet and trunk) and interface group configuration view

Usage Guidelines

None

Example

Reset STP statistics.

```
switch(config-100ge1/0/1)#stp reset statistic
switch(config-100ge1/0/1)#
```

7.3.13 stp revision-level

Function

The **stp revision-level** command is used to set the MSTP revision level.

Format

- **stp revision-level** { *range* | **default** }

Parameters

Parameters	Description	Value
range	Specifies the STP revision level.	The value is an integer in the range from 0 to 65535.
default	Indicates the default.	0

Default Value

The default STP revision level is 0.

View

STP configuration view

Usage Guidelines

You can use this command to set the STP revision level. The STP revision level, region name, and VLAN mapping table together determine the MST region to which the switch belongs.

Example

Set the STP revision level to 2.

```
switch(config-stp)#stp revision-level 2
switch(config-stp)#
```

7.3.14 stp root-guard

Function

The **stp root-guard** command is used to configure the root guard on a switch.

Format

- **stp root-guard** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the root guard.	-
disable	Disables the root guard.	-

Default Value

disable

View

Interface configuration view (Ethernet and trunk) and interface group configuration view

Usage Guidelines

None

Example

Enable the loop guard on a switch.

```
switch(config-100ge1/0/1)#stp root-guard enable
switch(config-100ge1/0/1)#
```

7.3.15 stp tc-flush-arp

Function

The **stp tc-flush-arp** command is used to enable or disable protection for TC-BPDU packets.

Format

- **stp tc-flush-arp** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables protection for TC-BPDU packets.	-
disable	Disables protection for TC-BPDU packets.	-

Default Value

disable

View

STP configuration view

Usage Guidelines

None

Example

Enable protection for TC-BPDU packets.

```
switch(config-100ge1/0/1)#stp root-guard enable
switch(config-100ge1/0/1)#
```

7.3.16 stp tc-hold-off

Function

The **stp tc-hold-off** command is used to set the topology change delay / suppression time for TC protection.

Format

- **stp tc-hold-off** { *time* | **default** }

Parameters

Parameters	Description	Value
time	Specifies the delay or suppression time.	The value is an integer in the range from 4 to 30 (unit: s).
default	Indicates the default.	10 seconds

Default Value

The default topology change delay / suppression time is 10 seconds.

View

STP configuration view

Usage Guidelines

In normal situations, upon receiving a TC-BPDU packet, the switch deletes the local MAC address entry and updates the ARP address table based on the STP instances in the updated MAC address table. When a user forges TC-BPDU packets to maliciously attack the switch, the switch receives a large number of TC-BPDU packets within a short period of time. The switch frequently deletes the local MAC address entries, resulting in frequent refresh of the ARP table. This affects spanning tree calculation and occupies lots of bandwidth resources, resulting in a high CPU usage. With TC-BPDU protection enabled, the switch deletes the local MAC address entry after receiving a TC-BPDU packet and starts a 10-second timer. If the switch receives TC-BPDU packets again within the timeout period, it deletes the MAC address entry for a maximum of six times only. This prevents frequent MAC address entry deletion and improves the network stability.
This command must be used together with the **stp tc-protection** command.

Example

Set the topology change delay / suppression time to 15 seconds.

```
switch(config-stp)#stp tc-hold-off 15
switch(config-stp)#
```

7.3.17 stp tc-protection

Function

The **stp tc-protection** command is used to enable or disable protection against TC-BPDU packet attacks.

Format

- **stp tc-protection** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables protection against TC-BPDU packet attacks of the spanning tree.	-
disable	Disables protection against TC-BPDU packet attacks of the spanning tree.	-

Default Value

By default, protection against TC-BPDU packet attacks is disabled.

View

STP configuration view

Usage Guidelines

The system starts the Hold-off timer for an interface after the interface receives a TC-BPDU, and drops received TC-BPDUs before the Hold-off timer times out. This function filters out redundant TC-BPDUs and protects the system against malicious attacks.

Example

Enable protection against TC-BPDU packet attacks.

```
switch(config-stp)#stp tc-protection enable
switch(config-stp)#
```

7.3.18 stp tc-protection threshold

Function

The **stp tc-protection threshold** command is used to set the threshold at which a device, after receiving such packets, processes packets indicating topology change per unit time and refreshes its forwarding table entries.

Format

- **stp tc-protection threshold** { *value* | **default** }

Parameters

Parameters	Description	Value
value	Specifies the threshold at which a device, after receiving such packets, processes packets indicating topology change per unit time and refreshes its forwarding table entries.	The value is an integer in the range from 1 to 255.
default	Indicates the default threshold.	2

Default Value

By default, the threshold for protection against TC-BPDU packet attacks is 2.

View

STP configuration view

Usage Guidelines

In a layer-2 network where the STP is running, a switch will delete MAC address table entries and ARP table entries after receiving packets indicating topology changes. Frequent deletion will affect the CPU greatly and may result in a high CPU usage.

By default, protection against topology change attacks is enabled for a switch. You can set the frequency at which a switch processes packets indicating topology changes per unit time. In a unit time, if receiving such packets for times greater than the configured threshold, the switch only handles packets for the times specified by the threshold. For those exceeding the threshold, after the timer times out, the switch handles them centrally once. This avoids frequent deletion of MAC address table entries and ARP table entries and thereby protects the switch.

Example

Set the threshold at which a switch processes TC-BPDU packets and refreshes forwarding table entries to 3.

```
switch(config-stp)#stp tc-protection threshold 3
```

```
switch(config-stp)#
```

7.3.19 stp timer-factor

Function

The **stp timer-factor** command is used to set the timeout multiplier of a spanning tree.

Format

- **stp timer-factor** { *timer-value* | **default** }

Parameters

Parameters	Description	Value
timer-value	Specifies the spanning tree timeout multiplier.	The value is an integer in the range from 1 to 20.
default	Indicates the default multiplier of time interval for sending Hello packets.	6

Default Value

6

View

STP configuration view

Usage Guidelines

None

Example

Set the timeout multiplier of a spanning tree.

```
switch(config-stp)#stp timer-factor 8
switch(config-stp)#
```

7.3.20 stp transmit-limit

Function

The **stp transmit-limit** command is used to set the number of times to send packets in a Hello Time interval of STP (that is, the number of BPDUs sent).

Format

- **stp transmit-limit** { *limit-value* | **default** }

Parameters

Parameters	Description	Value
limit-value	Specifies the number of BPDUs sent in a Hello interval of STP.	The value is an integer in the range from 1 to 10.
default	Indicates the default.	6

Default Value

By default, the number of BPDUs sent in a Hello interval is 6.

View

STP configuration view

Usage Guidelines

The more the BPDU packets sent in a Hello Time interval, the more the system resources are occupied. You can use this command to properly limit the BPDU packets sent in a Hello Time interval to avoid excessive bandwidth resource occupation during network topology flapping.

Example

Set the number of BPDUs sent in a Hello interval of STP to 2.

```
switch(config-stp)#stp transmit-limit 2
switch(config-stp)#
```

7.3.21 stp trap

Function

The **stp trap** command is used to enable or disable the STP trap.

Format

- **stp trap** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the STP trap.	-
disable	Disables the STP trap.	-

Default Value

By default, the STP trap is disabled.

View

STP configuration view

Usage Guidelines

None

Example

Enable the STP trap.

```
switch(config-stp)#stp trap enable
switch(config-stp)#
```

7.4 G.8032 Configuration Commands

7.4.1 g8032

Function

The **g8032** command is used to switch to the G.8032 configuration view from the global configuration view.

Format

- **g8032**

Description

None

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Switch to the G8032 configuration view from the global configuration view.

```
switch(config)#g8032
switch(config-g8032)#
```

7.4.2 g8032 instance mip-port

Function

The **g8032 instance mip-port** command configures a MIP port for a G.8032 instance.

Format

- **g8032 instance** *instance-num* **mip-port**

Parameters

Parameters	Description	Value
instance-num	Specifies the G.8032 instance number.	The value is an integer in the range from 1 to 16.

Default Value

None

View

Interface configuration view (Ethernet and trunk) and interface group configuration view

Usage Guidelines

None

Example

Configure a MIP port for the virtual channel UP MEP of the G.8032 instance.

```
switch(config-100ge1/0/1)#g8032 instance 1 mip-port
switch(config-100ge1/0/1)#
```

7.4.3 g8032 instance {port1|port2} (in the Interface Configuration View)

Function

The **g8032 instance {port1|port2}** command is used to configure an interface as port 1 or port 2 of a G.8032 instance.

Format

- **g8032 instance** *instance-num* { **port1** | **port2** }

Parameters

Parameters	Description	Value
instance-num	Specifies the G.8032 instance number.	The value is an integer in the range from 1 to 16.

Default Value

None

View

Interface configuration view (Ethernet and trunk) and interface group configuration view

Usage Guidelines

None

Example

Configure an interface as port 1 of a G.8032 instance.

```
switch(config-100ge1/0/1)#g8032 instance 1 port1
switch(config-100ge1/0/1)#
```

7.4.4 g8032 instance {add|remove} mip-port

Function

The **g8032 instance add mip-port** command adds a MIP port for the virtual channel UP MEP of the G.8032 instance.
The **g8032 instance remove mip-port** command removes a MIP port for the virtual channel UP MEP of the G.8032 instance.

Format

- **g8032 instance** *instance-num* **add mip-port** { **10gigaethernet** | **100gigaethernet** } *mip-port-number*
- **g8032 instance** *instance-num* **add mip-port eth-trunk** *trunk-number*
- **g8032 instance** *instance-num* **remove mip-port** { **10gigaethernet** | **100gigaethernet** } *mip-port-number*
- **g8032 instance** *instance-num* **remove mip-port eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
instance-num	Specifies the G.8032 instance number.	The value is an integer in the range from 1 to 16.
mip-port -number	Specifies an Ethernet interface number.	The value is an integer string in the range of <1-1>/<0-2>/<1-52>.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.

Default Value

None

View

G8032 configuration view

Usage Guidelines

None

Example

Add a MIP port 1/01 for the virtual channel UP MEP of the G.8032 instance.

```
switch(config-g8032)#g8032 instance 1 add mip-port 10gigaethernet 1/0/1
switch(config-g8032)#
```

7.4.5 g8032 instance {port1|port2} (in the G8032 Configuration View)

Function

The **g8032 instance {port1|port2}** command is used to configure port 1 and port 2 for the current G.8032 instance.
The **no g8032 instance {port1|port2}** command is used to delete port 1 and port 2 configured for the current G.8032 instance.

Format

- **g8032 instance** *instance-num* { **port1** | **port2** } { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **g8032 instance** *instance-num* { **port1** | **port2** } **eth-trunk** *trunk-number*
- **no g8032 instance** *instance-num* { **port1** | **port2** }

Parameters

Parameters	Description	Value
instance-num	Specifies the G.8032 instance number.	The value is an integer in the range from 1 to 16.
interface-number	Specifies an Ethernet interface number.	The value is an integer string in the range of <1-1>/<0-2>/<1-52>.
trunk-number	Specifies a trunk interface number.	The value is an integer in the range from 1 to 32.

Default Value

None

View

G8032 configuration view

Usage Guidelines

None

Example

Configure Port 1 of the G.8032 instance.

```
switch(config-g8032)#g8032 instance 1 port1 10gigaethernet 1/0/1
switch(config-g8032)#
```

7.4.6 g8032 instance {port1|port2} fs

Function

The **g8032 instance {port1|port2} fs** command is used to trigger a forcible switchover on a port of a G.8032 instance.

Format

- **g8032 instance** *instance-number* { **port1** | **port2** } **fs**

Parameters

Parameters	Description	Value
instance-number	Specifies the G.8032 instance number.	The value is an integer in the range from 1 to 16.

Default Value

None

View

G8032 configuration view

Usage Guidelines

G8032 version v1 do not support this command.

Example

Configure forcible switching for the G.8032 instance.

```
switch(config)#g8032
switch(config-g8032)#g8032 instance 1 channel 1
switch(config-g8032)#g8032 instance 1 port1 10gigaethernet 1/0/1
switch(config-g8032)#g8032 instance 1 port1 fs
switch(config-g8032)#
```

7.4.7 g8032 instance {port1|port2} ms

Function

The **g8032 instance {port1|port2} ms** command is used to trigger a manual switchover on a port of a G.8032 instance.

Format

- **g8032 instance** *instance-number* { **port1** | **port2** } **ms**

Parameters

Parameters	Description	Value
instance-number	Specifies the instance number.	The value is an integer in the range from 1 to 16.

Default Value

None

View

G8032 configuration view

Usage Guidelines

G8032 version v1 do not support this command.

Example

Configure manual switching for the G.8032 instance.

```
switch(config-g8032)#g8032 instance 2 port1 ms
switch(config-g8032)#
```

7.4.8 g8032 instance channel

Function

The **g8032 instance channel** command is used to configure a control channel for the current G.8032 instance.

Format

- **g8032 instance** *instance-number* **channel** *channel-number*

Parameters

Parameters	Description	Value
instance-number	Specifies the instance number.	The value is an integer in the range from 1 to 16.
channel-number	Specifies the control channel number.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

G8032 configuration view

Usage Guidelines

None

Example

Configure the control channel 1 for the G.8032 instance.

```
switch(config-g8032)#g8032 instance 1 channel 1
switch(config-g8032)#
```

7.4.9 g8032 instance clear

Function

The **g8032 instance clear** command is used to clear the state of a G.8032 instance.

Format

- **g8032 instance** *instance-number* **clear**

Parameters

Parameters	Description	Value
instance-num	Specifies the G.8032 instance number.	The value is an integer in the range from 1 to 16.

Default Value

None

View

G8032 configuration view

Usage Guidelines

None

Example

Clear the state of G.8032 instance 1.

```
switch(config-g8032)#g8032 instance 1 clear
switch(config-g8032)#
```

7.4.10 g8032 instance mel

Function

The **g8032 instance mel** command is used to configure the protocol channel hierarchy for the G.8032 instance.

Format

- **g8032 instance** *instance-num* **mel** *mel-num*

Parameters

Parameters	Description	Value
instance-num	Specifies the G.8032 instance number.	The value is an integer in the range from 1 to 16.
mel-num	Specifies the G.8032 instance protocol channel hierarchy.	The value is an integer in the range from 0 to 7.

Default Value

None

View

G8032 configuration view

Usage Guidelines

None

Example

Set the G.8032 instance protocol channel hierarchy to 6 levels.

```
switch(config-g8032)#g8032 instance 1 mel 6
switch(config-g8032)#
```

7.4.11g8032 instance mode

Function

The **g8032 instance mode** command is used to configure the revertive or non-revertive node mode for a G.8032 instance.

Format

- **g8032 instance** *instance-number* **mode** { **revertive** | **non-revertive** }

Parameters

Parameters	Description	Value
instance-number	Specifies the instance number.	The value is an integer in the range from 1 to 16.
(revertive|non-revertive)	Specifies the node mode of G.8032 instance, including revertive or non-revertive.	-

Default Value

revertive

View

G8032 configuration view

Usage Guidelines

None

Example

View information about users who have logged in and are configured the switch.

```
switch(config-g8032)#g8032 instance 1 mode revertive
switch(config-g8032)#
```

7.4.12 g8032 instance role

Function

The **g8032 instance role** command is used to configure a node role for a G.8032 instance.

Format

- **g8032 instance** *instance-number* **role** { **rpl-owner-node** | **neighbor** | **none** }

Parameters

Parameters	Description	Value
instance-number	Specifies the instance number.	The value is an integer in the range from 1 to 16.
(rpl-owner-node|neighbor|none)	Specifies the node role of a G.8032 instance.	-

Default Value

None

View

G8032 configuration view

Usage Guidelines

None

Example

Set the node role of the G.8032 instance to rpl-owner-node.

```
switch(config-g8032)#g8032 instance 1 role rpl-owner-node
switch(config-g8032)#
```

7.4.13 g8032 instance rpl

Function

The **g8032 instance rpl** command is used to configure an RPL interface for a G.8032 instance.

Format

- **g8032 instance** *instance-number* **rpl** { **port1** | **port2** | **none** }

Parameters

Parameters	Description	Value
instance-number	Specifies the instance number.	The value is an integer in the range from 1 to 16.

Parameters	Description	Value
(port1|port2|none)	Specifies the RPL port of a G.8032 instance.	-

Default Value

None

View

G8032 configuration view

Usage Guidelines

None

Example

Set the RPL port of a G.8032 instance to port 1.

```
switch(config-g8032)#g8032 instance 1 rpl port1
switch(config-g8032)#
```

7.4.14 g8032 instance vc-holdoff-timer

Function

The **g8032 instance vc-holdoff-timer** command is used to set the hold-off timer for virtual channels of a G.8032 instance (in the unit of milliseconds).

Format

- **g8032 instance** *instance-num* **vc-holdoff-timer** { *vc-holdoff-timer* | **default** }

Parameters

Parameters	Description	Value
instance-num	Specifies the G.8032 instance number.	The value is an integer in the range from 1 to 16.
vc-holdoff-timer	Specifies the hold-off timer period (ms).	The value is an integer in the range from 0 to 10000.
default	Indicates the default.	0 ms

Default Value

0 ms

View

G8032 configuration view

Usage Guidelines

None

Example

Set the virtual channel hold-off timer of a G.8032 instance to 100 ms.

```
switch(config-g8032)#g8032 instance 1 vc-holdoff-timer 100
switch(config-g8032)#
```

7.4.15 g8032 instance vc-mel

Function

The **g8032 instance vc-mel** command configures the virtual channel hierarchy for the G.8032 instance.

Format

- **g8032 instance** *instance-num* **vc-mel** *vc-mel-num*

Parameters

Parameters	Description	Value
instance-num	Specifies the G.8032 instance number.	The value is an integer in the range from 1 to 16.
vc-mel-num	Configure the virtual channel hierarchy of a G.8032 instance.	The value is an integer in the range from 0 to 7.

Default Value

None

View

G8032 configuration view

Usage Guidelines

None

Example

Set the G.8032 instance virtual channel hierarchy to Level 1.

```
switch(config-g8032)#g8032 instance 1 vc-mel 1
switch(config-g8032)#
```

7.4.16 g8032 instance vc-mep {port1|port2|none}

Function

The **g8032 instance vc-mep {port1|port2|none}** command is used to configure the MEP port of the virtual channel for a G.8032 instance.

Format

- **g8032 instance** *instance-num* **vc-mep** { **port1** | **port2** | **none** }

Parameters

Parameters	Description	Value
instance-num	Specifies the G.8032 instance number.	The value is an integer in the range from 1 to 16.

Default Value

None

View

G8032 configuration view

Usage Guidelines

None

Example

Set the MEP port of the virtual channel of a G.8032 instance to port1.

```
switch(config-g8032)#g8032 instance 1 vc-mep port1
switch(config-g8032)#
```

7.4.17 g8032 instance version

Function

The **g8032 instance version** command is used to set the G.8032 instance version number.

Format

- **g8032 instance** *instance-number* **version** { **v1** | **v2** }

Parameters

Parameters	Description	Value
instance-number	Specifies the instance number.	The value is an integer in the range from 1 to 16.

Default Value

v2

View

G8032 configuration view

Usage Guidelines

None

Example

Set the G.8032 instance version to v1.

```
switch(config-g8032)#g8032 instance 4 version v1
switch(config-g8032)#
```

7.4.18 g8032 instance virtual-channel

Function

The **g8032 instance virtual-channel** command is used to configure a virtual channel for a G.8032 instance.

Format

- **g8032 instance** *instance-number* **virtual-channel** *virtual-channel-number*

Parameters

Parameters	Description	Value
instance-number	Specifies the instance number.	The value is an integer in the range from 1 to 16.
virtual-channel-number	Specifies the virtual channel number of a G.8032 instance.	The value is an integer in the range from 0 to 4094.

Default Value

None

View

G8032 configuration view

Usage Guidelines

Setting the number of a virtual channel to 0 means deleting this virtual channel.

Example

Set the virtual channel number of the G.8032 instance to 1.

```
switch(config-g8032)#g8032 instance 1 virtual-channel 1
```

```
switch(config-g8032)#
```

7.4.19 g8032 instance vlan

Function

The **g8032 instance vlan** command is used to specify a mapping VLAN list for a G.8032 instance.
The **no g8032 instance vlan** command is used to delete a mapping VLAN list of a G.8032 instance.

Format

- **g8032 instance** *instance-number* **vlan** *vlan-list*
- **no g8032 instance** *instance-number* **vlan** *vlan-list*

Parameters

Parameters	Description	Value
instance-number	Specifies the instance number.	The value is an integer in the range from 1 to 16.
vlan-list	Specifies the VLAN list.	The value is a string of characters, such as 1, 3, 5-10.

Default Value

None

View

G8032 configuration view

Usage Guidelines

None

Example

Configure a mapping VLAN list for a G.8032 instance.

```
switch(config-g8032)#g8032 instance 1 vlan 1,3,5-10
switch(config-g8032)#
```

Delete the VLAN list mapped to a G.8032 instance.

```
switch(config-g8032)#no g8032 instance 1 vlan 1,3,5-10
switch(config-g8032)#
```

7.4.20 g8032 instance wtr-timer

Function

The **g8032 instance wtr-timer** command is used to set the WTR timer interval for a G.8032 instance.

Format

- **8032 instance** *instance-number* **wtr-timer** { *wtr-timer* | **default** }

Parameters

Parameters	Description	Value
instance-number	Specifies the instance number.	The value is an integer in the range from 1 to 16.
wtr-timer	Specifies the WTR timer interval of a G.8032 instance.	The value is an integer in the range from 1 to 12, in minutes.
default	Indicates the default.	The default is 5 minutes.

Default Value

The default WTR timer interval of a G.8032 instance is 5 minutes.

View

G8032 configuration view

Usage Guidelines

None

Example

Set the WTR timer interval of a G.8032 instance to 10 minutes.

```
switch(config-g8032)#g8032 instance 1 wtr-timer 10
switch(config-g8032)#
```

7.4.21 g8032 instance guard-timer

Function

The **g8032 instance guard-timer** command is used to set the Guard-Timer interval for a G.8032 instance.

Format

- **g8032 instance** *instance-number* **guard-timer** { *guard-timer* | **default** }

Parameters

Parameters	Description	Value
instance-number	Specifies the instance number.	The value is an integer in the range from 1 to 16.
guard-timer	Specifies the Guard-Timer interval.	The value is an integer in the range from 10 to 2000, in milliseconds.
default	Indicates the default timer.	500 ms

Default Value

The default Guard-Timer interval of a G8032 instance is 500 ms.

View

G8032 configuration view

Usage Guidelines

None

Example

Set the Guard-Timer interval of a G8032 instance to 1000 ms.

```
switch(config-g8032)#g8032 instance 1 guard-timer 1000
switch(config-g8032)#
```

7.4.22 g8032 instance hold-off-timer

Function

The **g8032 instance hold-off-timer** command is used to set the Hold-off-Timer interval for a G.8032 instance.

Format

- **g8032 instance** *instance-number* **hold-off-timer** { *hold-off-timer* | **default** }

Parameters

Parameters	Description	Value
instance-number	Specifies the instance number.	The value is an integer in the range from 1 to 16.
hold-off-timer	Specifies the Hold-off-Timer interval.	The value is an integer in the range from 0 to 10000, in milliseconds.
default	Indicates the default.	0 ms

Default Value

The default Hold-off-Timer interval of a G8032 instance is 0 ms.

View

G8032 configuration view

Usage Guidelines

None

Example

Set the Hold-off-Timer interval of a G8032 instance to 2000 ms.

```
switch(config-g8032)#g8032 instance 1 hold-off-timer 2000
switch(config-g8032)#
```

7.4.23 g8032 trap {enable|disable}

Function

The **g8032 trap {enable|disable}** command is used to enable or disable the G.8032 alarm function.

Format

- **g8032 trap** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the G.8032 alarm function.	-
disable	Disables the G.8032 alarm function.	-

Default Value

enable

View

G8032 configuration view

Usage Guidelines

None

Example

Enable the G.8032 alarm function.

```
switch(config-g8032)#g8032 trap enable
switch(config-g8032)#
```

7.4.24 g8032 vs-switch {enable|disable}

Function

The **g8032 vs-switch {enable|disable}** command is used to enable or disable the virtual link switch.

Format

- **g8032 vs-switch** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the virtual link switch.	-
disable	Disables the virtual link switch.	-

Default Value

disable

View

G8032 configuration view

Usage Guidelines

On a multi-ring network, the virtual link switch should be disabled. The virtual link switch needs no configuration on a single-ring network.

Example

Enable the virtual link switch.

```
switch(config-g8032)#g8032 vs-switch enable
switch(config-g8032)#
```

7.4.25 no g8032 instance

Function

The **no g8032 instance** command is used to delete a G.8032 instance.

Format

- **no g8032 instance** *instance-num*

Parameters

Parameters	Description	Value
instance-num	Specifies the G.8032 instance number.	The value is an integer in the range from 1 to 16.

Default Value

None

View

G8032 configuration view

Usage Guidelines

None

Example

Delete G.8032 instance 1.

```
switch(config-g8032)#no g8032 instance 1
switch(config-g8032)#
```

7.4.26 show g8032

Function

The **show g8032** command is used to show all G.8032 information.

Format

- **show g8032**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, G.8032 configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

None

Example

Show all G.8032 information.

```
switch#show g8032
g8032 trap:enable
g8032 vs-switch:disable
switch#
```

7.4.27 show g8032 instance

Function

The **show g8032 instance** command shows information about a certain G.8032 instance or all G.8032 instances.

Format

- **show g8032 instance** *instance-num*
- **show g8032 instance**

Parameters

Parameters	Description	Value
instance-num	Specifies the G.8032 instance number.	The value is an integer in the range from 1 to 16.

Default Value

None

View

Common user view, privileged user view, global configuration view, G.8032 configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

None

Example

Show information about G.8032 instance 1.

```
switch#show g8032 instance 1
g8032 trap:enable
g8032 vs-switch:disable
  The g8032 instance does not exist.
switch#
```

Show all G.8032 instance information.

```
switch#show g8032 instance
g8032 trap:enable
g8032 vs-switch:disable
switch#
```

7.4.28 show g8032 instance interface

Function

The **show g8032 instance** command is used to show interface information of a G.8032 instance.

Format

- **show g8032 instance** *instance-num* **interface**
- **show g8032 instance interface**

Parameters

Parameters	Description	Value
instance-num	Specifies the G.8032 instance number.	The value is an integer in the range from 1 to 16.

Default Value

None

View

Common user view, privileged user view, global configuration view, G.8032 configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

None

Example

Show interface information of a G.8032 instance.

```
switch#show g8032 instance interface
Instance Interface      Type    Operate   Forward     Rx-Count  Tx-Count
1        10ge-1/0/2     rpl     working   blocking    0         50
1        10ge-1/0/2     normal  working   forwarding  0         50
switch#
```

7.4.29 show g8032 interface

Function

The **show g8032 interface** command is used to show G.8032 interface information.

Format

- **show g8032 interface**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, G.8032 configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

None

Example

Show G.8032 interface information.

```
switch#show g8032 interface
Instance Interface        Type      Operate    Forward       Rx-Count   Tx-Count
1        10ge-1/0/1       normal    working    forwarding    0          0
switch#
```

7.5 UDLD Configuration Commands

7.5.1 udld work-mode

Function

The **udld work-mode** command is used to set the detection mode of a unidirectional link.

Format

- **udld work-mode** { **normal** | **aggressive** }

Parameters

Parameters	Description	Value
normal	Indicates the normal mode.	-
aggressive	Indicates the aggressive mode.	-

Default Value

Normal

View

Global configuration view

Usage Guidelines

None

Example

Set the detection mode of a unidirectional link.

```
switch(config)#udld work-mode aggressive
switch(config)#
```

7.5.2 udld uni-shutdown

Function

The **udld uni-shutdown** command is used to set the shutdown mode of a unidirectional path interface.

Format

- **udld uni-shutdown** { **manual** | **auto** }

Parameters

Parameters	Description	Value
manual	The interface is shut down manually.	-
auto	The interface is shut down automatically.	-

Default Value

auto

View

Global configuration view

Usage Guidelines

None

Example

Set the shutdown mode of a unidirectional path interface.

```
switch(config)#udld uni-shutdown manual
switch(config)#
```

7.5.3 udld advertise-interval

Function

The **udld advertise-interval** command is used to set the transmission interval of Advertisement packets.

Format

- **udld advertise-interval** { *adver-interval* | **default** }

Parameters

Parameters	Description	Value
adver-interval	Specifies the Advertisement packet transmission interval.	The value is an integer in the range from 2 to 15 (unit: s).
default	Uses the default Advertisement packet transmission interval.	7 seconds

Default Value

7 seconds

View

Global configuration view

Usage Guidelines

None

Example

Set the transmission interval of Advertisement packets.

```
switch(config)#udld advertise-interval 8
switch(config)#
```

7.5.4 udld trap {enable|disable}

Function

The **udld trap{enable|disable}** command is used to enable or disable the UDLD alarm function.

Format

- **udld trap** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the UDLD alarm function.	-
disable	Disables the UDLD alarm function.	-

Default Value

By default, the UDLD alarm function is disabled.

View

Global configuration view

Usage Guidelines

None

Example

Enable the UDLD alarm function.

```
switch(config)#udld trap enable
switch(config)#
```

7.5.5 udld {enable|disable}

Function

The **udld {enable|disable}** command is used to enable or disable the UDLD protocol at an interface.

Format

- **udld** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the UDLD protocol at an interface.	-
disable	Disables the UDLD protocol at an interface.	-

Default Value

By default, the UDLD protocol is disabled at an interface.

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

None

Example

Enable the UDLD protocol at an interface.

```
switch(config-100ge1/0/1)#udld enable
switch(config-100ge1/0/1)#
```

7.5.6 udld aggressive {enable|disable}

Function

The **udld aggressive {enable|disable}** command is used to enable or disable the UDLD aggressive mode at an interface.

Format

- **udld aggressive** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the UDLD aggressive mode at an interface.	-

Parameters	Description	Value
disable	Disables the UDLD aggressive mode at an interface.	-

Default Value

By default, the UDLD aggressive mode at an interface is disabled.

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

None

Example

Enable the UDLD aggressive mode at an interface.

```
switch(config-100ge1/0/1)#udld aggressive enable
switch(config-100ge1/0/1)#
```

7.5.7 show udld local

Function

The **show udld local** command is used to show local UDLD information.

Format

- **show udld local**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Show local UDLD information.

```
switch(config)#show udld local
```

```
switch(config)#
```

7.5.8 show udld interface

Function

The **show udld interface** command is used to show UDLD interface information.

Format

- **show udld interface**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Show UDLD interface information.

```
switch(config)#show udld interface
switch(config)#
```

7.5.9 show udld peer

Function

The **show udld peer** command is used to show UDLD peer information.

Format

- **show udld peer**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Show UDLD peer information.

```
switch(config)#show udld peer
switch(config)#
```

7.5.10 show udld config

Function

The **show udld config** command is used to show the UDLD configuration.

Format

- **show udld config**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Show the UDLD configuration.

```
switch(config)#show udld config
switch(config)#
```

7.6 FLINK Configuration Commands

7.6.1 join mlink group

Function

The **join mlink group** adds an interface to a Monitor Link group and configures the interface as an uplink or downlink interface.
The **no join mlink group** command removes an interface from the corresponding Monitor Link group.

Format

- **join mlink group** *mlink-group-number* **role** { **uplink** | **downlink** }
- **no join mlink group** *mlink-group-number*

Parameters

Parameters	Description	Value
mlink-group-number	Specifies a Monitor Link group number.	The value is an integer ranging from 1 to 16.
uplink	Sets the interface as the uplink member interface of the Monitor Link group.	-
downlink	Sets the interface as the downlink member interface of the Monitor Link group.	-

Default Value

By default, a Monitor Link group does not have any interface

View

Interface configuration view (Ethernet and trunk)

Usage Guidelines

A Monitor Link group consists of uplinks and downlinks. One Monitor Link group can have multiple uplinks and downlinks. All downlinks monitor the state of the uplinks. Once all uplinks are faulty, all downlinks will be forcibly disabled. When any uplink restores, all downlinks are enabled again. The changes of the downlink state do not affect the uplink state.
The Monitor Link group configuration rules are as follows:
One interface can be the uplink interface of multiple Monitor Link groups.
One interface can be the downlink interface of only one Monitor Link group.
One interface cannot be an uplink interface and a downlink interface simultaneously
If an interface is added to the eth-trunk, it cannot be added to the Monitor Link group.

Example

Add interface 10gigaethernet 1/0/1 to Monitor Link group 1 and configure it as an uplink interface.

```
switch(config-10ge1/0/1)#join mlink group 1 role uplink
switch(config-10ge1/0/1)#
```

7.6.2 join flink group

Function

The **join flink group** command adds an interface to a Resilient Link group and configures the interface as a master, slave, or sender interface.
The **no join flink group** command removes an interface from the corresponding Resilient Link group.

Format

- **join flink group** *flink-group-number* **role** { **master** | **slave** | **sender** }
- **no join flink group** *flink-group-number*

Parameters

Parameters	Description	Value
flink-group-number	Specifies a Resilient Link group number.	The value is an integer ranging from 1 to 16.
master	Configures the interface as a master interface in the Resilient Link group.	-
slave	Configures the interface as a slave interface in the Resilient Link group.	-
sender	Configures the interface as a sender interface in the Resilient Link group.	-

Default Value

By default, the Resilient Link group does not have any interface.

View

Interface configuration view (Ethernet and trunk)

Usage Guidelines

Before running this command, activate the Resilient Link group. Otherwise, the interface cannot be successfully added to the group.
The Resilient Link group configuration rules are as follows:
If MSTP is enabled on an interface, the interface cannot be added to the Resilient Link group
If an interface is added to the eth-trunk, it cannot be added to the Resilient Link group.

Warning: Two uplinks must be monitored by the BFD or Monitor link. Otherwise, the master and slave interfaces may fail to correctly identify the faulty link, resulting in link loop on the master and slave interfaces after the link state restores.

Example

Add interface 10gigaethernet 1/0/1 to Resilient Link group 1 and configure the interface as the master interface.

```
switch(config-10ge1/0/1)#join flink group 1 role master
switch(config-10ge1/0/1)#
```

7.6.3 manual-change

Function

The **manual-change** command configures the manual active/standby link switching of a Resilient Link group

Format

- **manual-change**

Parameters

None

Default Value

None

View

RLINK configuration view

Usage Guidelines

In addition to active/standby link switching automatically triggered by diversified types of faults, you can use the NMS command to trigger link switching, that is, manual link switching.
On the condition that the link state permits, you can use the NMS command to forcibly set a port in the Resilient Link group to the BLK or FWD state. Then, other port is set to the corresponding FWD or BLK state. According to different Resilient Link group types, manual link switching is classified into single-point ode and dual-point mode.
The following conditions must be met to achieve active/standby switching:
The Resilient Link group must have master and slave interfaces.
The link must allow forced switching. That is, both the master and slave links must be in the linkup state. (For example, when the master is FWD and the slave is BLK, if you want to change the master to BLK and the slave to FWD state, make sure the slave link is in the linkup state.)
After this command is executed, temporary packet loss may occur during link switching, at an level of milliseconds.

Example

Manually implement active/standby switching.

```
switch(config-flink1)#manual-change
switch(config-flink1)#
```

7.6.4 mlink group

Function

The **mlink group** command creates a Monitor Link group and accesses its configuration view. If the Monitor Link group already exists, the system directly accesses its configuration view.
The **no mlink group** command removes an existing Monitor Link group.

Format

- **mlink group** *mlink-group-number*
- **no mlink group** *mlink-group-number*

Parameters

Parameters	Description	Value
mlink-group-number	Specifies a Monitor Link group number.	The value is an integer ranging from 1 to 16.

Default Value

By default, no Monitor Link group exists.

View

Global configuration view

Usage Guidelines

The Monitor Link group is mainly used for monitoring the uplink to perfect the Resilient Link group backup function.

Example

Create Monitor Link group 1.

```
switch(config)#mlink group 1
switch(config-mlink1)#
```

Delete Monitor Link group 1.

```
switch(config)#no mlink group 1
switch(config)#
```

7.6.5 add interface {10gigaethernet|100gigaethernet } role {master|slave|sender}

Function

The **add interface {10gigaethernet|100gigaethernet} role {master|slave|sender}** command adds an interface to a Resilient Link group and configures the interface as a master, slave, or sender interface.
The **no interface {10gigaethernet|100gigaethernet}** command removes an interface from the corresponding Resilient Link group.

Format

- **add interface** { **10gigaethernet** | **100gigaethernet** } *interface-number* **role** { **master** | **slave** | **sender** }
- **add interface eth-trunk** *trunk-number* **role** { **master** | **slave** | **sender** }
- **no interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **no interface eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer. The value is <1-1>/<0-2>/<1-52>.
trunk-number	Specifies a trunk interface number.	The value is an integer ranging from 1 to 32

Default Value

By default, the Resilient Link group does not have any interface.

View

RLINK configuration view

Usage Guidelines

One interface can be added to only one port-based Resilient Link group. However, one interface can be added to multiple VLAN-based Resilient Link groups. One interface cannot be added to the port-based Resilient Link group and VLAN-based Resilient Link group simultaneously.
The Resilient Link group configuration rules are as follows:
If MSTP is enabled on an interface, the interface cannot be added to the Resilient Link group.
If an interface is added to the eth-trunk, it cannot be added to the Resilient Link group.

Warning: Two uplinks must be monitored by the BFD or Monitor link. Otherwise, the master and slave interfaces may fail to correctly identify the faulty link, resulting in link loop on the master and slave interfaces after the link state restores.

Example

Add interface 10gigaethernet 1/0/1 to Resilient Link group 1 and configures the interface as the master interface.

```
switch(config-flink1)#add interface 10gigaethernet 1/0/1 role master
switch(config-flink1)#
```

7.6.6 add interface {10gigaethernet|100gigaethernet|ethernet| xgigaethernet } role {uplink|downlink}

Function

The **add interface {10gigaethernet|100gigaethernet} role {uplink|downlink}** adds an interface to a Monitor Link group and configures the interface as an uplink or downlink interface.
The **no interface {10gigaethernet|100gigaethernet}** command removes an interface from the corresponding Monitor Link group.

Format

- **add interface** { **10gigaethernet** | **100gigaethernet** } *interface-number* **role** { **uplink** | **downlink** }
- **add interface eth-trunk** *trunk-number* **role** { **uplink** | **downlink** }
- **no interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **no interface eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
interface-number	Specifies the interface number.	The value is an integer. the value is <1-1>/<0-2>/<1-52>.
trunk-number	Specifies a trunk interface number.	The value is an integer ranging from 1 to 124

Default Value

By default, the Monitor Link group does not have any interface

View

MLINK configuration view

Usage Guidelines

One interface can be configured as the uplink interface in multiple Monitor Link groups. However, it can be configured as the downlink interface in only one Monitor Link group. One interface cannot be an uplink interface and a downlink interface simultaneously.
The Monitor Link group configuration rules are as follows:
One interface can be the uplink interface of multiple Monitor Link groups.
One interface can be the downlink interface of only one Monitor Link group.
One interface cannot be an uplink interface and a downlink interface simultaneously.
If an interface is added to the eth-trunk, it cannot be added to the Monitor Link group

Example

Add interface 10gigaethernet 1/0/1 to Monitor Link group 1 and configures it as an uplink interface.

```
switch(config-mlink1)#add interface 10gigaethernet 1/0/1 role uplink
switch(config-mlink1)#
```

7.6.7 protect-vlan

Function

The **protect-vlan** command configures the protection VLAN of a RLINK instance.
The **no protect-vlan** command deletes the protection VLAN of a RLINK instance.

Format

- **protect-vlan** *vlan-list*
- **no protect-vlan** *vlan-list*

Parameters

Parameters	Description	Value
vlan-list	Specifies the protection VLAN list.	The value is an integer ranging from 1 to 4094, for example, 1, 3, and 10-20.

Default Value

None

View

RLINK configuration view

Usage Guidelines

If a protection VLAN is configured, for master port A, the VLAN is in the FWD state. For slave port B, the VLAN is in the BLK state. When the link connected to master port A is faulty, the slave port B is switched to the FWD state.

Example

Configure VLAN 100 as the protection VLAN of the RLINK instance.

```
switch(config-flink1)#protect-vlan 100
switch(config-flink1)#
```

7.6.8 receive-timeout

Function

The **receive-timeout** command configures multiples of the timeout value for the Resilient Link group to receive protocol packets from the peer.

Format

- **receive-timeout** { *timeout-value* | **default** }

Parameters

Parameters	Description	Value
timeout-value	Configures multiples of the timeout value to receive protocol packets from the peer.	The value is an integer ranging from 3 to 50. It is a multiple of send-interval.
default	Configures the default multiples of the timeout value to receive protocol packets from the peer.	In dual-point mode, the default is 15 seconds. In single-point mode, the default is 0 seconds.

Default Value

None

View

RLINK configuration view

Usage Guidelines

If the actual timeout value to receive protocol packets from the peer exceeds the multiples x interval for sending packets on the peer (the default is 1 second), you can configure the timeout value using the send-interval command.
After this command is executed, if no protocol packet is received from the peer within the timeout time, the switch considers that the peer does not have local ports in FWD state. The timeout value configured using this command will affect the switching performance. Exercise caution when using this command.

Example

Set the timeout value for a Resilient Link group to receive protocol packets from the peer to 16 seconds.

```
switch(config-flink1)#receive-timeout 16
switch(config-flink1)#
```

7.6.9 reverse {enable|disable}

Function

The **reverse {enable|disable}** command enables or disables Resilient Link group failback.

Format

- **reverse** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables Resilient Link group failback.	-
disable	Disables Resilient Link group failback	-

Default Value

By default, Resilient Link group failback is disabled

View

RLINK configuration view

Usage Guidelines

Generally, when the active link in the Resilient Link restores to be normal, to maintain traffic stability, the active link is in the BLK state and does not perform preemption. If you want to restore it to the active link, you can use the following two methods:
Enable Resilient Link group failback. The active link will automatically switch back after the failback timer expires. You can set the failback interval using the reverse-time command.
Forcibly switch back the link using the manual-change command.

Example

Enable the failback function of Resilient Link group 1.

```
switch(config-flink1)#reverse enable
switch(config-flink1)#
```

7.6.10 reverse time

Function

The **reverse time** command configures the failback time of the Resilient Link group.

Format

- **reverse time** { *time-value* | **default** }

Parameters

Parameters	Description	Value
time-value	Configures the failback time of the Resilient Link group	The value is an integer ranging from 3 to 60, in seconds.
default	Configures the default fail back time of the Resilient Link group	15 seconds

Default Value

By default, the failback time of the Resilient Link group is 15 seconds.

View

RLINK configuration view

Usage Guidelines

Failback indicates that a link does not switch back to a restored master port immediately after the fault disappears. The link switches back to the master port after a period of time. This delay is known as failback time.
If the network is unstable or has a lower delay requirements, the failback time can be set to a larger value to avoid smooth switching.

Example

Set the failback time of Resilient Link group 1 to 60 seconds.

```
switch(config-flink1)#reverse time 60
switch(config-flink1)#
```

7.6.11flink group

Function

The **flink group** command creates a Resilient Link group and accesses its configuration view. If the Resilient Link group already exists, the system directly accesses its configuration view.
The **no flink group** command removes an existing Resilient Link group.

Format

- **flink group** *flink-group-number*
- **no flink group** *flink-group-number*

Parameters

Parameters	Description	Value
flink-group-number	Specifies the Resilient Link group number.	The value is an integer ranging from 1 to 16,

Default Value

By default, no Resilient Link group exists.

View

Global configuration view

Usage Guidelines

None

Example

Create Resilient Link group 1.

```
switch(config)#flink group 1
switch(config-flink1)#
```

Delete existing Resilient Link group 1.

```
switch(config)#no flink group 1
switch(config)#
```

7.6.12 flink group send-vlan

Function

The **flink group send-vlan** command configures the VLAN ID of the Tx RLINK protocol packet.

Format

- **flink group** *flink-group-number* **send-vlan** *vlan-id*

Parameters

Parameters	Description	Value
flink-group-number	Specifies the Resilient Link group number.	The value is an integer ranging from 1 to 16,

Parameters	Description	Value
vlan-id	Configures the VLAN ID of the Tx RLINK protocol packet.	The value is an integer ranging from 1 to 4094.

Default Value

None

View

Interface configuration view (Ethernet and trunk)

Usage Guidelines

In dual-point mode, you must configure the VLAN for sending protocol packets, that is, Tx VLAN. The VLAN ID must belong to either of the VLAN groups of the ports sending and receiving packets. Otherwise, packets may not be normally received by dual nodes.
Before using this command, run the flink group command to create a Resilient Link group and activate it. Then, run the add interface {10gigaethernet|100gigaethernet} role {master|slave|sender} or join flink group command to add the port to the Resilient Link group. Otherwise, the configuration fails and the system prompts "%Failed to get flink member status!"

Example

Set the VLAN ID of the Tx RLINK protocol packet to VLAN 1.

```
switch(config-10ge1/0/1)#flink group 1 send-vlan 1
switch(config-10ge1/0/1)#
```

7.6.13 send-interval

Function

The **send-interval** command configures the interval for sending protocol packets.

Format

- **send-interval** { *time-interval* | **default** }

Parameters

Parameters	Description	Value
time-interval	Specifies the interval for sending packets.	The value is an integer ranging from 1000 to 10000, in milliseconds.
default	Specifiesthe default interval for sending packets.	In dual-point mode, the default is 1000 ms. In single-point mode, the default is 0 ms.

Default Value

In dual-point mode, the default is 1000 ms. In single-point mode, the default is 0 ms.

View

RLINK configuration view

Usage Guidelines

None

Example

Set the interval for sending protocol packets of the Resilient Link group to 3 seconds.

```
switch(config-flink1)#send-interval 3000
switch(config-flink1)#
```

7.6.14 show mlink config

Function

The **show mlink config** command shows the configuration file information of the uplink monitoring function.

Format

- **show mlink config**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

None

Example

Display the configuration file information of the uplink monitoring function.

```
switch#show mlink config
Version: MLINK_VB3.00.01.00
 mlink group 1
```

```
 interface 10ge-1/0/1
 join mlink group 1 role uplink
switch#
```

7.6.15 show mlink group

Function

The **show mlink group** command shows the information of all Monitor Link groups or the designated Monitor Link group.

Format

- **show mlink group**
- **show mlink group** *mlink-group-number*

Parameters

Parameters	Description	Value
mlink-group-number	Specifies a Monitor Link group number. It is optional.	The value is an integer ranging from 1 to 16

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

After the Monitor Link group is created and an uplink port or a downlink port is added, you can use this command to view information about the Monitor Link group, including the member interface name, member interface state, and interface link state.

Example

Display information about Monitor Link group 1.

```
switch#show mlink group

Mlink group 1 information:
  Group status: active
  Snmp trap : disable

  Member                Role       State      Status     Linkstate
  10ge-1/0/1            UPLINK     BLOCK      ACTIVE     up/down
switch#
```

7.6.16 show mlink interface

Function

The **show mlink interface** command shows configuration information of all Monitor Link interfaces or a specified interface.

Format

- **show mlink interface**
- **show mlink interface** { **10gigaethernet** |**100gigaethernet** } *interface-number*
- **show mlink interface eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
interface-number	Specifies the interface number.	The value is an integer. the value is <1-1>/<0-2>/<1-52>.
trunk-number	Specifies a trunk interface number.	The value is an integer ranging from 1 to 124.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

None

Example

Display the Monitor Link configuration of interface 10gigaethernet 1/0/1.

```
switch#show mlink interface 10gigaethernet 1/0/1
Interface   Group   Role   State Status     Linkstate
10ge-1/0/1      1    UPLINK   BLOCK    ACTIVE    up/down
switch#
```

7.6.17 show flink config

Function

The **show flink config** command shows the configuration file information of the dual-uplink redundancy function.

Format

- **show flink config**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

None

Example

Display the configuration file information of the dual-uplink redundancy function.

```
switch#show flink config
Version: RLINK_VB3.00.02.00
flink group 1
flink group 2
switch#
```

7.6.18 show flink group

Function

The **show flink group** command shows the information of all Resilient Link groups or the designated Resilient Link group

Format

- **show flink group**
- **show flink group** *flink-group-number*

Parameters

Parameters	Description	Value
flink-group-number	Specifies the Resilient Link group number. It is optional.	The value is an integer ranging from 1 to 16.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

You can use this command to show the Resilient Link group state information, including the group state, group type, failback time, and member interface. When the Resilient Link group is faulty, you can locate the fault by analyzing the state information

Example

Display state information of Resilient Link group 1.

```
switch#show flink group 1
Rlink group 1 information:
  Group status              : active
  Group type                : single
  Group vlanlist            : N/A
  Reverse                   : disable
  Snmp trap                 : disable
switch#
```

7.6.19 show flink interface

Function

The **show flink interface** command shows configuration information of all Resilient Link interfaces or a specified interface.

Format

- **show flink interface**
- **show flink interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **show flink interface eth-trunk** *trunk-number*

Parameters

Parameters	Description	Value
interface-number	Specifies the interface number.	The value is an integer. the value is <1-1>/<0-2>/<1-52>.
trunk-number	Specifies a trunk interface number	The value is an integer ranging from 1 to 32.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

None

Example

Display configuration information of all Resilient Link interfaces.

```
switch#show flink interface
Interface    Group     Role    State Status       Linkstate
10ge-1/0/1       2      MASTER     BLOCK      ACTIVE      down/down
switch#
```

7.6.20 type {single|double}

Function

The **type {single|double}** command sets the single-point mode or dual-point mode for a Resilient Link group..

Format

- **type** { **single** | **double** }

Parameters

Parameters	Description	Value
single	Sets the Resilient Link group o work in single-point mode.	-
double	Sets the Resilient link group to work in dual-point mode.	-

Default Value

By default, a Resilient Link group works in single-point mode.

View

RLINK configuration view

Usage Guidelines

If a Resilient Link group is activated, you cannot modify its working mode.

Example

Set Resilient Link group 1 to work in dual-point mode.

```
switch(config-flink1)#type double
```

```
switch(config-flink1)#
```

7.6.21 snmp-trap {enable|disable}

Function

The **snmp-trap {enable|disable}** command enables or disables the Resilient Link or Monitor Link alarm function.

Format

- **snmp-trap** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	enables the trap alarm function.	-
disable	disable the trap alarm function.	-

Default Value

By default, this function is disabled

View

RLINK configuration view, MLINK configuration view

Usage Guidelines

None

Example

Enables the trap alarm function for the Monitor Link.

```
switch(config-mlink1)#snmp-trap enable
switch(config-mlink1)#
```

7.7 BFD Configuration Commands

7.7.1 bfd authentication

Function

The **bfd authentication** command configures the password for BFD plain-text authentication or Key ID and key for MD5 authentication.
The **no bfd authentication** command disables the authentication.

Format

- **bfd authentication md5** *key-id key-string*
- **bfd authentication text** *simple-password*

- **no bfd authentication**

Parameters

Parameters	Description	Value
key-id	Specifies the key ID for the MD5 authentication.	The value is an integer ranging from 1 to 255.
key-string	Specifies the key for the MD5 authentication.	The value is a character string.
simple-password	Specifies the password for the plain-text authentication.	The value is a string of characters without spaces.

Default Value

None

View

Interface configuration view (Ethernet and trunk), VLANIF configuration view, Loopback configuration view, and interface group configuration view

Usage Guidelines

Simple password authentication: Each node is configured with one or more passwords (each password corresponds to one ID). A password is contained in the transmitted control packet. The receiving node checks the received packet based on the own configuration.
MD5 authentication: One node is configured with one or more keys (each key corresponds to one ID). The sent packet contains MD5 abstract information corresponding to a key instead of the key. To avoid repeated attacks, a BFD packet contains a SN. For MD5 authentication, this SN can be increased.

Example

Configure the plain-text authentication for BFD and set the password to feisutest at interface 10gigaethernet.

```
switch(config-10ge1/0/1)#bfd authentication text feisutest
switch(config-10ge1/0/1)#
```

7.7.2 bfd {enable|disable}

Function

The **bfd {enable|disable}** command enables or disables the BFD protocol.

Format

- **bfd** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	enables BFD at an interface	-
disable	disable BFD at an interface	-

Default Value

By default, the interface BFD protocol is disabled

View

Interface configuration view (Ethernet and trunk), VLANIF configuration view, Loopback configuration view, and interface group configuration view

Usage Guidelines

None

Example

Enable the BFD protocol at interface 10gigaethernet1/0/1.

```
switch(config-10ge1/0/1)#bfd enable
switch(config-10ge1/0/1)#
```

7.7.3 bfd min-echo

Function

The **bfd min-echo** command configures the minimum interval for receiving ECHO packets.

Format

- **bfd min-echo** *echo-interval*

Parameters

Parameters	Description	Value
echo-interval	Specifies the minimum interval for receiving ECHO packets.	The value is an integer ranging from 0 to 1000. 0 indicates that the echo function is disabled, in milliseconds.

Default Value

By default, the echo function is disabled

View

Interface configuration view (Ethernet and trunk), VLANIF configuration view, Loopback configuration view, and interface group configuration view

Usage Guidelines

BFD detection is classified into asynchronous detection mode and on-demand detection mode. The echo function is an additional function of two detection modes

When the echo function is enabled, a node sends a series of BFD ECHO packets to a neighbor, and the neighbor reflects the packets to the transmit node. If no response ECHO packet is received within a period of time (or a large amount of ECHO packets are lost), the notification session is disabled. The echo function is applicable to the asynchronous detection mode and on-demand detection mode. When using the echo function, ECHO packets are used for fault detection to decrease the BFD control packet speed (asynchronous mode) or completely stop sending BFD control packets (on-demand mode).

Compared with the echo function, the pure asynchronous mode has an advantage: To reach the same detection duration, the number of BFD control packets used in asynchronous mode is half of that used in the ECHO function. If the echo function cannot be used, the asynchronous mode must be adopted.

The advantage of echo function is that this function detects forwarding path of the neighbor only. This can decrease the round trip time jitter, shorten the detection, and detect faults that cannot be detected by other methods.

The echo function can be independently enabled in two directions. Precondition for enabling the echo function in a specific direction: The node that implements the echo reflection must indicate the capability of providing the echo function; the node that sends ECHO packets must indicate the will of implementing the echo function.

Example

Set the minimum interval for receiving echo packets to 300 ms.

```
switch(config-10ge1/0/1)#bfd min-echo 300
switch(config-10ge1/0/1)#
```

7.7.4 bfd min-tx min-rx multiplier

Function

The **bfd min-tx min-rx multiplier** command configures the minimum interval for sending packets, minimum interval for receiving packets, and detection expiration times of BFD

Format

- **bfd min-tx** *tx-interval* **min-rx** *rx-interval* **multiplier** *timeout-multiple*

Parameters

Parameters	Description	Value
tx-interval	Specifies the minimum interval for sending packets.	The value is an integer ranging from 100 to 1000, in milliseconds.
rx-interval	Specifies the minimum interval for receiving packets.	The value is an integer ranging from 100 to 1000, in milliseconds.
timeout-multiple	Specifies the timeout multiple times of detection.	The value is an integer ranging from 1 to 255.

Default Value

None.

View

Interface configuration view (Ethernet and trunk), VLANIF configuration view, Loopback configuration view, and interface group configuration view

Usage Guidelines

None

Example

Set tx-interval to 300 ms, rx-interval to 300 ms, and timeout-multiple to 5.

```
switch(config-10ge1/0/1)#bfd min-tx 300 min-rx 300 multiplier 5
switch(config-10ge1/0/1)#
```

7.7.5 bfd role

Function

The **bfd role** command sets the BFD role to active or passive.

Format

- **bfd role** { **active** | **passive** }

Parameters

Parameters	Description	Value
active	Indicates the active mode.	-
passive	Indicates the passive mode.	-

Default Value

By default, the BFD role is in active mode.

View

Interface configuration view (Ethernet and trunk), VLANIF configuration view, Loopback configuration view, and interface group configuration view

Usage Guidelines

In the initialization phase of the BFD session establishment process, the active role or passive role is determined by the application. However, at least one end must be active

Example

Set the BFD role of interface 10gigaethernet 1/0/1 to passive.

```
switch(config-10ge1/0/1)#bfd role passive
```

```
switch(config-10ge1/0/1)#
```

7.7.6 bfd {start|stop}

Function

The **bfd {start|stop}** command globally enables or disables the BFD.

Format

- **bfd** { **start** | **stop** }

Parameters

Parameters	Description	Value
start	Globally enables the BFD.	-
stop	Globally disables the BFD.	-

Default Value

By default, the BFD is disabled globally.

View

Global configuration view

Usage Guidelines

Before configuring basic BFD functions, you must configure the VLAN and IP address for the interface. If network-layer connectivity needs to be detected, you need to configure the routing protoco

Example

Globally enable the BFD.

```
switch(config)#bfd start
switch(config)#
```

7.7.7 bfd trap

Function

The **bfd trap** command enables or disables the BFD session state alarm (Up or Down)

Format

- **bfd trap** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	enables the BFD alarm.	-
disable	disables the BFD alarm..	-

Default Value

By default, the BFD alarm function is disabled.

View

Global configuration view

Usage Guidelines

None

Example

Enable the BFD alarm.

```
switch(config)#bfd trap enable
switch(config)#
```

7.7.8 bfd track

Function

The **bfd track** command adds a static BFD session based on IPv4 or IPv6.

Format

VLANIF configuration view:

- **bfd track** *track-number* **remote-ip** *ipv4-address1* **local-ip** *ipv4-address2*
- **bfd track** *track-number* **remote-ip** *ipv4-address1* **local-ip** *ipv4-address2* **one-arm-echo**
- **bfd track** *track-number* **remote-ip6** *ipv6-address1* **local-ip6** *ipv6-address2*
- **bfd track** *track-number* **remote-ip6** *ipv6-address1* **local-ip6** *ipv6-address2* **one-arm-echo**
- **no bfd track** *track-number*

Global configuration view:

- **bfd track** *track-number* **vlan** *vlan-id* **remote-ip** *ipv4-address1* **local-ip** *ipv4-address2*
- **bfd track** *track-number* **vlan** *vlan-id* **remote-ip** *ipv4-address1* **local-ip** *ipv4-address2* **one-arm-echo**
- **bfd track** *track-number* **vlan** *vlan-id* **remote-ip6** *ipv6-address1* **local-ip** *ipv6-address2*
- **bfd track** *track-number* **vlan** *vlan-id* **remote-ip6** *ipv6-address1* **local-ip** *ipv6-address2* **one-arm-echo**
- **no bfd track** *track-number*
- **no bfd track** *all*

Parameters

Parameters	Description	Value
track-number	Specifies the static BFD session ID.	The value is an integer ranging from 1 to 64.
ipv4-address1	Specifies a remote IPv4 address.	The value is in dotted decimal notation.
ipv4-address2	Specifies a local IPv4 address.	The value is in dotted decimal notation.
ipv6-address1	Specifies a remote IPv6 address.	-
vlan-id	Specifies a VLAN entry.	The value is an integer ranging from 1 to 4094.
ipv6-address2	Specifies a local IPv6 address.	-

Default Value

None

View

VLANIF configuration view and global configuration view

Usage Guidelines

None

Example

In VLAN1 interface configuration, configure the track information of remote address 1.1.1.1 and local address 2.2.2.2.

```
switch((config-vlanif-1)#bfd track 1 remote-ip 1.1.1.1 local-ip 2.2.2.2
switch((config-vlanif-1)#
```

In VLAN1 interface configuration, configure the track information of remote address 1::1 and local address 2::2.

```
switch(config-vlanif-1)#bfd track 1 remote-ip6 1::1 local-ip6 2::2
switch(config-vlanif-1)#
```

7.7.9 show bfd config

Function

The **show bfd config** command shows BFD session configuration information.

Format

- **show bfd config**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet, trunk, and Loopback), VLANIF configuration view, and interface group configuration view

Usage Guidelines

None

Example

Display BFD session configuration information.

```
switch#show bfd config
Version                          :BFD_VX2.10.00.00
 bfd start

interface 10ge-1/0/5
 bfd enable
switch#
```

7.7.10 show bfd interface

Function

The **show bfd interface** command shows information about an interface with BFD enabled.

Format

- **show bfd interface**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet, trunk, and Loopback), VLANIF configuration view, and interface group configuration view

Usage Guidelines

None

Example

Display information of interface 10gigaethernet 1/0/1 after BFD is enabled.

```
switch(config)#show bfd interface
  Interface: 10ge-1/0/1
  Version: v1.0
  Role: active
  Mode: asynch
  Echo State: disabled
  Min out interval(ms): 1000
  Min in interval(ms): 1000
  Multiplier: 3
  Authentication: disabled

switch(config)#
```

7.7.11show bfd session

Function

The **show bfd session** command shows information of a dynamically established BFD session

Format

- **show bfd session**
- **show bfd session** { **include** | **exclude** | **begin** } **substring** *string*
- **show bfd session verbose**

Parameters

Parameters	Description	Value
string	Specifies a matching character string.	The value is a character string.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet, trunk, and Loopback), VLANIF configuration view, and interface group configuration view

Usage Guidelines

Generally, OSPF or BGP generates sessions by dynamically triggering BFD.

Example

Display information of a dynamically established BFD session (using two connected switchs as an example).

```
switch#show bfd session
Interface: 10ge1/0/1
Version: v1.0
Role: active
Mode: asynch
Operate Mode: asynch-without-echo
Local Discriminator: 1
Remote Discriminator: 1
Diagnose: 0
Echo State: disabled
Min tx interval: 200
Min rx interval: 200
Multiplier: 3
Negotiate interval: 200
Negotiate echo interval: 0
Negotiate multiplier: 3
Session State: up
Session Addr: 00:00:02:98:10:1d
Authentication: disabled
```

7.7.12 show bfd track

Function

The **show bfd track** command shows static BFD session information.

Format

- **show bfd track**
- **show bfd track** { **include** | **exclude** | **begin** } **substring** *string*
- **show bfd track** *track-number*

Parameters

Parameters	Description	Value
track-number	Specifies the static BFD session ID.	The value is an integer ranging from 1 to 64.
string	Specifies a matching character string.	The value is a character string.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet, trunk, and Loopback), VLANIF configuration view, and interface group configuration view

Usage Guidelines

Static BFD sessions are mainly used for VRRP association.

Example

Display static BFD session information.

```
switch#show bfd track
TrackIndex    Interface       Remote-bind    Local-addr SessionDiscr    SessionState
1             10ge-1/0/1      N/A            00:00:02:90:04:04  1       failure
switch#
```

7.8 VRRP Configuration Commands

7.8.1 ip vrrp

Function

The **ip vrrp** command is used to create a VRRP record entry. (This command applies to IPv4 networks.)
The **no ip vrrp** command is used to delete a VRRP record entry.

Format

- **ip vrrp** *virtual-route-id*
- **no ip vrrp** [*virtual-route-id*]

Parameters

Parameters	Description	Value
virtual-route-id	Specifies the global ID of a virtual router.	The value is an integer in the range from 1 to 255.

Default Value

None

View

VLANIF configuration view

Usage Guidelines

Before configuring a virtual router, you must create a record and specify the ID of the virtual router.

Example

Create a VRRP record entry in VLAN 10 configuration view.

```
switch(config)#interface vlan 10
switch(config-vlanif-10)#ip address 1.1.1.1/24
switch(config-vlanif-10)#ip vrrp 1
switch(config-vlanif-10)#
```

7.8.2 ip vrrp snmp-trap {enable|disable}

Function

The **ip vrrp snmp-trap {enable|disable}** command is used to enable or disable the SNMP trap.

Format

- **ip vrrp snmp-trap** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the SNMP trap.	-
disable	Disables the SNMP trap.	-

Default Value

By default, the SNMP trap is enabled.

View

Global configuration view

Usage Guidelines

When the VRRP state changes, the switch sends the corresponding VRRP state alarm if the SNMP trap is enabled.

Example

Disable the SNMP trap.

```
switch(config)#ip vrrp snmp-trap disable
switch(config)#
```

7.8.3 ip vrrp advertise-interval

Function

The **ip vrrp advertise-interval** command is used to set the interval for sending VRRP notification packets. (This command applies to IPv4 networks.)

Format

- **ip vrrp** *virtual-route-id* **advertise-interval** { *interval-time* | **default** }

Parameters

Parameters	Description	Value
virtual-route-id	Specifies the global ID of a virtual router.	The value is an integer in the range from 1 to 255.
interval-time	Specifies the interval for sending packets.	The value is an integer in the range from 1 to 40 (unit: s).
default	Indicates the default.	1 second

Default Value

By default, the interval for sending VRRP notification packets is 100 centiseconds (1 second).

View

VLANIF configuration view

Usage Guidelines

A short interval ensures high VRRP sensitivity. This can shorten the time to switch over between master and backup virtual routers and reduce data loss. A long interval can relieve the load on networks.

Example

Set the interval for sending VRRP notification packets to 10s.

```
switch(config)#interface vlan 10
switch(config-vlanif-10)#ip vrrp 1 advertise-interval 10
switch(config-vlanif-10)#
```

7.8.4 ip vrrp associate-address

Function

The **ip vrrp associate-address** command is used to set the IP address associated with a virtual router. (This command applies to IPv4 networks.)
The **no ip vrrp associate-address** command is used to delete the IP address associated with a virtual router.

Format

- **ip vrrp** *virtual-route-id* **associate-address** *ip-address*
- **ip vrrp** *virtual-route-id* **associate-address** *ip-address* **primary**
- **no ip vrrp** *virtual-route-id* **associate-address** *ip-address*

Parameters

Parameters	Description	Value
virtual-route-id	Specifies the global ID of a virtual router.	The value is an integer in the range from 1 to 255.
ip-address	Specifies the IP address associated with a	The value is in dotted decimal

Parameters	Description	Value
	virtual router.	notation.

Default Value

None

View

VLANIF configuration view

Usage Guidelines

After a virtual router record is created, you need to configure at least one associated IP address as the default gateway address of the terminal host. After the VRRP is enabled, the switch checks this IP address. If this address is the same as the IP address of a physical port, the switch always regards this port as a master virtual router port (setting the priority of this address to the maximum number 255 automatically).

Example

Set the IP address associated with the VRRP to 10.255.255.254.

```
switch (config)#interface vlan 10
switch (config-vlanif-10)#ip vrrp 1 associate-address 10.255.255.254
switch (config-vlanif-10)#
```

7.8.5 ip vrrp authentication-mode

Function

The **ip vrrp authentication-mode** command is used to specify the authentication mode and key of a VRRP instance.

Format

- **ip vrrp** *virtual-route-id* **authentication-mode** { **simple** | **md5** } { **cipher** | **plain** } *key*
- **ip vrrp** *virtual-route-id* **authentication-mode** { **simple** | **md5** } *key*
- **no ip vrrp** *virtual-route-id* **authentication-mode**

Parameters

Parameters	Description	Value
virtual-route-id	Specifies the global ID of a virtual router.	The value is an integer in the range from 1 to 255.
key	Specifies the key corresponding to the VRRP instance authentication mode.	The value is a string of characters. The maximum length is 8 bytes.
simple	Indicates the simple character authentication mode.	-
md5	Indicates the MD5 authentication mode.	-

Default Value

None

View

VLANIF configuration view

Usage Guidelines

None

Example

Set the authentication mode of VRRP backup group 1 at interface VLANIF 10 to simple character authentication, and the key to fstest.

```
switch (config)#interface vlan 10
switch (config-vlanif-10)# ip vrrp 1 associate-address 10.255.255.254
switch (config-vlanif-10)#ip vrrp 1 authentication-mode simple fstest
```

7.8.6 ip vrrp check-ttl {enable|disable}

Function

The **ip vrrp check-ttl {enable|disable}** command is used to enable or disable the TTL detection for VRRP notification packets.

Format

- **ip vrrp** *vrrp-id* **check-ttl** { **enable** | **disable** }

Parameters

Parameters	Description	Value
vrrp-id	Specifies a virtual router ID.	The value is an integer in the range from 1 to 255.
enable	Enables the TTL detection for VRRP notification packets.	-
disable	Disables the TTL detection for VRRP notification packets.	-

Default Value

By default, the TTL detection for VRRP notification packets is disabled.

View

VLANIF configuration view

Usage Guidelines

None

Example

Enable the TTL detection for VRRP notification packets.

```
switch(config-vlanif-2)#ip vrrp 2 check-ttl enable
switch(config-vlanif-2)#
```

7.8.7 ip vrrp gratuitous-arp {enable|disable}

Function

The **ip vrrp gratuitous-arp {enable|disable}** command enables or disables the master VRRP interface to periodically send gratuitous ARP packets.

Format

- **ip vrrp** *vrrp-id* **gratuitous-arp** { **enable** | **disable** }

Parameters

Parameters	Description	Value
vrrp-id	Specifies a virtual router ID.	The value is an integer in the range from 1 to 255.
enable	Enables the master VRRP interface to periodically send gratuitous ARP packets.	-
disable	Disables the master VRRP interface to periodically send gratuitous ARP packets.	-

Default Value

By default, the master VRRP interface is enabled to periodically send gratuitous ARP packets.

View

VLANIF configuration view

Usage Guidelines

None

Example

Disable the master VRRP interface to periodically send gratuitous ARP packets.

```
switch(config-vlanif-2)#ip vrrp 2 gratuitous-arp disable
switch(config-vlanif-2)#
```

7.8.8 ip vrrp gratuitous-arp timeout

Function

The **ip vrrp gratuitous-arp timeout** command is used to set a timeout period (an interval) for the master VRRP interface to send gratuitous ARP packets.

Format

- **ip vrrp** *vrrp-id* **gratuitous-arp timeout** { *time* | **default** }

Parameters

Parameters	Description	Value
vrrp-id	Specifies a virtual router ID.	The value is an integer in the range from 1 to 255.
time	Specifies a timeout period for sending gratuitous ARP packets.	The value is an integer in the range from 30 to 1200, in seconds.
default	Indicates the default.	300 seconds

Default Value

300 seconds

View

VLANIF configuration view

Usage Guidelines

To enable other connected NEs to learn its address, a VRRP backup group needs to actively send gratuitous ARP packets. The set interval at which the master VRRP interface sends gratuitous ARP packets should be shorter than the address aging period of the NEs.

Example

Set the timeout period to 180s for the master VRRP interface to send gratuitous ARP packets.

```
switch(config-vlanif-10)#ip address 1.1.1.1/24
switch(config-vlanif-10)#ip vrrp 1 gratuitous-arp enable
switch(config-vlanif-10)#ip vrrp 1 gratuitous-arp timeout 180
switch(config-vlanif-10)#
```

7.8.9 ip vrrp holding-multiplier

Function

The **ip vrrp holding-multiplier** command is used to set the timeout multiplier for changing the state of an associated virtual interface from backup to master.

Format

- **ip vrrp** *vrrp-id* **holding-multiplier** { *time* | **default** }

Parameters

Parameters	Description	Value
vrrp-id	Specifies a virtual router ID.	The value is an integer in the range from 1 to 255.
time	Specifies the timeout multiplier.	The value is an integer in the range from 3 to 10 (unit: times).
default	Uses the default.	3

Default Value

3

View

VLANIF configuration view

Usage Guidelines

None

Example

Set the timeout multiplier for changing the state of an associated virtual interface from backup to master to 1.

```
switch(config-vlanif-10)#ip vrrp 1
switch(config-vlanif-10)#ip vrrp 1 holding-multiplier 5
switch(config-vlanif-10)#
```

7.8.10 ip vrrp preempt

Function

The **ip vrrp preempt** command is used to enable or disable VRRP preemption.

Format

- **ip vrrp** *virtual-route-id* **preempt** { **enable** | **disable** }

Parameters

Parameters	Description	Value
virtual-route-id	Specifies the global ID of a virtual router.	The value is an integer in the range from 1 to 255.

Default Value

By default, VRRP preemption is enabled.

View

VLANIF configuration view

Usage Guidelines

If you want to enable a switch with a higher priority to actively become the master, configure VRRP preemption for the switch.

Example

Disable the VRRP preemption mode.

```
switch(config)#interface vlan 10
switch(config-vlanif-10)#ip vrrp 1 preempt disable
switch(config-vlanif-10)#
```

7.8.11ip vrrp preempt timer delay

Function

The **ip vrrp preempt timer delay** command is used to set the preemption delay for a switch in the VRRP backup group.

Format

- **ip vrrp** *virtual-route-id* **preempt timer delay** { *delay-value* | **default** }

Parameters

Parameters	Description	Value
virtual-route-id	Specifies a VRRP backup group ID.	The value is an integer in the range from 1 to 255.
delay-value	Specifies the preemption delay, in seconds.	The value is an integer in the range from 0 to 3600.
default	Specifies the default preemption delay time.	0 seconds

Default Value

By default, the preemption delay is set to 0s, that is, immediate preemption.

View

VLANIF configuration view

Usage Guidelines

If you want to enable a switch with a higher priority to actively become the master, configure VRRP preemption for the switch.

Example

Set the VRRP preemption delay to 3s.

```
switch(config)#interface vlan 10
switch(config-vlanif-10)#ip vrrp 1 preempt timer delay 3
switch(config-vlanif-10)#
```

7.8.12 ip vrrp priority

Function

The **ip vrrp priority** command is used to set the priority for VRRP master virtual router election. (This command applies to IPv4 networks.)

Format

- **ip vrrp** *virtual-route-id* **priority** { *priority* | **default** }

Parameters

Parameters	Description	Value
virtual-route-id	Specifies the global ID of a virtual router.	The value is an integer in the range from 1 to 255.
priority	Specifies the priority for VRRP master virtual router election.	The value is an integer in the range from 1 to 254.
default	Indicates the default priority.	100

Default Value

The default of priority is 100.

View

VLANIF configuration view

Usage Guidelines

The priority is the most important Parameters used by the VRRP to elect a master virtual router. The priority ranges from 1 to 254. When none of the VRRP routers forming a virtual router is a permanent master virtual router (the physical port IP addresses of all routers are different from the associated IP address), the VRRP router with the highest priority is elected as the master virtual router.

Example

Set the priority for VRRP master virtual router election to 200.

```
switch(config)#interface vlan 10
switch(config-vlanif-10)#ip vrrp 1 priority 200
switch(config-vlanif-10)#
```

7.8.13 ip vrrp role admin

Function

The **ip vrrp role admin** command is used to create a management VRRP backup group.
The **no ip vrrp role admin** command is used to delete a management VRRP backup group.

Format

- **ip vrrp** *virtual-route-id* **role admin**
- **no ip vrrp** *virtual-route-id* **role admin**

Parameters

Parameters	Description	Value
virtual-route-id	Specifies a VRRP backup group ID.	The value is an integer in the range from 1 to 255.

Default Value

By default, no management VRRP backup group is created.

View

VLANIF configuration view

Usage Guidelines

None

Example

Create a management VRRP backup group.

```
switch(config-vlanif-1)#ip vrrp 1 role admin
switch(config-vlanif-1)#
```

7.8.14 ip vrrp track admin-vrrp interface vlan

Function

The **ip vrrp track admin-vrrp interface vlan** command is used to configure an interface listened by the management VRRP.
The **no ip vrrp track admin-vrrp interface vlan** command is used to delete an interface listened by the management VRRP.

Format

- **ip vrrp** *virtual-route-id* **track admin-vrrp interface vlan** *vlan-id virtual-route-id*
- **no ip vrrp** *virtual-route-id* **track admin-vrrp interface vlan** *vlan-id virtual-route-id*

Parameters

Parameters	Description	Value
virtual-route-id	Specifies a VRRP backup group ID.	The value is an integer in the range from 1 to 255.
vlan-id	Specifies a VLANIF interface number.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

VLANIF configuration view

Usage Guidelines

None

Example

Configure an interface listened by the management VRRP.

```
switch(config-vlanif-1)#ip vrrp 2 track admin-vrrp interface vlan 1 1
switch(config-vlanif-1)#
```

7.8.15 ip vrrp track bfd-session

Function

The **ip vrrp track bfd-session** command is used to bind a BFD session and a VRRP instance to achieve a fast switchover. The **no ip vrrp track bfd-session** command is used to release a binding.

Format

- **ip vrrp** *virtual-route-id* **track bfd-session** *bfdsession-id*
- **ip vrrp** *virtual-route-id* **track bfd-session** *bfdsession-id* { **increased** | **reduced** } { *priority-value* | **default** }
- **no ip vrrp** *virtual-route-id* **track bfd-session** *bfdsession-id*

Parameters

Parameters	Description	Value
virtual-route-id	Specifies the global ID of a virtual router.	The value is an integer in the range from 1 to 255.
Bfd-session-id	Specifies the instance number of a BFD session.	The value is an integer in the range from 1 to 500.
priority-value	Specifies the priority increase or decrease value when the listened BFD session state changes to Down.	The value is an integer in the range from 1 to 255.

Parameters	Description	Value
default	Indicates the default priority increase or decrease value.	10

Default Value

None

View

VLANIF configuration view

Usage Guidelines

Before using this command, ensure that the BFD session instance exists.

Example

Bind VRRP instance 1 with BFD session instance 1.

```
switch(config)#interface vlan 10
switch(config-vlanif-10)#ip vrrp 1 track bfd-session 1
switch(config-vlanif-10)#
```

7.8.16 ip vrrp track interface vlan

Function

The **ip vrrp track interface vlan** command is used to bind an associated VLAN interface (applicable to IPv4).
The **no ip vrrp track interface vlan** command is used to unbind from an associated VLAN interface.

Format

- **ip vrrp** *virtual-route-id* **track interface vlan** *vlan-id*
- **ip vrrp** *virtual-route-id* **track interface vlan** *vlan-id* { **increased** | **reduced** } { *priority-value* | **default** }
- **no ip vrrp** *virtual-route-id* **track interface vlan** *vlan-id*

Parameters

Parameters	Description	Value
virtual-route-id	Specifies the global ID of a virtual router.	The value is an integer in the range from 1 to 255.
vlan-id	Specifies the VLAN ID to be bound.	The value is an integer in the range from 1 to 4094.
priority-value	Specifies the priority increase or decrease value when the listened BFD session state changes to Down.	The value is an integer in the range from 1 to 255.
default	Indicates the default priority increase or decrease value.	10

Default Value

None

View

VLANIF configuration view

Usage Guidelines

You can use this command to associate a VLAN interface with a VRRP group. When the VLAN state becomes **Down**, the VRRP can detect the failure in a timely manner.

Example

Bind an associated VLAN interface.

```
switch(config-vlanif-10)#ip vrrp 1 track interface vlan 10
switch(config-vlanif-10)#
```

7.8.17 ip vrrp admin-vrrp associate-vrrp interface vlan

Function

The **ip vrrp admin-vrrp associate-vrrp interface vlan** command is used to configure a member VRRP backup group associated with the management VRRP.
The **no ip vrrp admin-vrrp associate-vrrp interface vlan** command is used to delete a member VRRP backup group associated with the management VRRP.

Format

- **ip vrrp admin-vrrp** *virtual-route-id1* **associate-vrrp interface vlan** *vlan-id virtual-route-id2*
- **no ip vrrp admin-vrrp** *virtual-route-id1* **associate-vrrp interface vlan** *vlan-id virtual-route-id2*

Parameters

Parameters	Description	Value
virtual-route-id1	Specifies the management VRRP backup group ID.	The value is an integer in the range from 1 to 255.
vlan-id	Specifies a VLANIF interface number.	The value is an integer in the range from 1 to 4094.
virtual-route-id2	Specifies the associated VRRP backup group ID.	The value is an integer in the range from 1 to 255.

Default Value

None

View

VLANIF configuration view

Usage Guidelines

None

Example

Configure a member VRRP backup group associated with the management VRRP.

```
switch(config-vlanif-1)#ip vrrp 1
switch(config-vlanif-1)#ip vrrp admin-vrrp 1 associate-vrrp interface vlan 1 3
switch(config-vlanif-1)#
```

7.8.18 reset ip vrrp statistic

Function

The **reset ip vrrp statistic** command is used to reset the global VRRP statistics.

Format

- **reset ip vrrp statistic**

Description

None

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Reset the global VRRP statistics.

```
switch(config)#reset ip vrrp statistic
switch(config)#
```

7.8.19 show ip vrrp

Function

The **show ip vrrp** command is used to show the IPv4 VRRP configuration.

Format

- **show ip vrrp**
- **show ip vrrp** { **include** | **exclude** | **begin** } **substring** *string*

Parameters

Parameters	Description	Value
string	Specifies a matching character string.	The value is a character string.

Default Value

None

View

Common user view, privileged user view, global configuration view, and VLANIF configuration view

Usage Guidelines

You can use this command to view the VLAN interface, VRRP ID, VRRP state, and priority of the IPv4 VRRP.

Example

Show the IPv4 VRRP configuration.

```
switch#show ip vrrp
  Interface      VRID Version VR-State Pri IP-Count State    Auth-Mode Auth-Key
  vlan 100       1    2       Initial  100 0        Active   none      N/A
  vlan 100       2    3       Initial  100 0        Active   none      N/A
switch#
```

7.8.20 show ip vrrp admin-vrrp

Function

The **show ip vrrp admin-vrrp** command is used to show the management VRRP configuration.

Format

- **show ip vrrp admin-vrrp**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, and VLANIF configuration view

Usage Guidelines

None

Example

Show the management VRRP configuration.

```
switch(config)#show ip vrrp admin-vrrp
  Admin-Interface          Admin-VRID      VR-State
  10ge-1/0/1                  1              Initial
  10ge-1/0/1                  1              Initial
  10ge-1/0/1                  1              Initial
switch(config)#
```

7.8.21 show ip vrrp associate interface

Function

The **show ip vrrp associate interface** command is used to show information about an interface associated with the VRRP.

Format

- **show ip vrrp associate interface**
- **show ip vrrp associate interface** { **include** | **exclude** | **begin** } **substring** *string*

Parameters

Parameters	Description	Value
string	Specifies a matching character string.	The value is a character string.

Default Value

None

View

Common user view, privileged user view, global configuration view, and VLANIF configuration view

Usage Guidelines

None

Example

Show information about an interface associated with the VRRP.

```
switch#show ip vrrp associate interface
  localIf          vrId          peerIf
  vlan 101          1             vlan 100
switch#
```

7.8.22 show ip vrrp binding

Function

The **show ip vrrp binding** command is used to show VRRP binding information.

Format

- **show ip vrrp binding**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, and VLANIF configuration view

Usage Guidelines

You can use this command to show the VRRP binding information, as shown in the following table.

Item	Description
Admin-Interface	Type and number of a management VRRP interface.
Admin-VRID	Management VRRP backup group ID.
Member-Interface	The interface type and number of the member VRRP backup group bound with the management VRRP.
Member-VRID	ID of the member VRRP backup group bound with the management VRRP.

Example

Show VRRP binding information.

```
switch#show ip vrrp binding
  Admin-Interface      Admin-VRID      Member-Interface      Member-VRID
  10ge-1/0/1                1              10ge-1/0/1                2
  10ge-1/0/1                1              10ge-1/0/1                3
  10ge-1/0/1                1              10ge-1/0/2                1
switch#
```

7.8.23 show ip vrrp binding admin-vrrp interface

Function

The **show ip vrrp binding admin-vrrp interface** command is used to show the binding between the management VRRP backup group and the member VRRP backup group.

Format

- **show ip vrrp binding admin-vrrp interface vlan** *vlan-id virtual-route-id*

Parameters

Parameters	Description	Value
vlan-id	Specifies a VLANIF interface number.	The value is an integer in the range from 1 to 4094.
virtual-route-id	Specifies the member VRRP backup group ID.	The value is an integer in the range from 1 to 255.

Default Value

None

View

Common user view, privileged user view, global configuration view, and VLANIF configuration view

Usage Guidelines

You can use this command to show the VRRP binding information, as shown in the following table.

Item	Description
Member-Interface	Type and number of a member VRRP interface.
Member-VRID	Member VRRP backup group ID.
VR-State	Member VRRP backup group state, including Master, Backup, and Initial.

Example

Show the binding between the management VRRP backup group and the member VRRP backup group.

```
switch#show ip vrrp binding admin-vrrp interface vlan 1 2
  Member-Interface              Member-VRID      VR-State
  vlan-1                        2                Initial
switch#
```

7.8.24 show ip vrrp config

Function

The **show ip vrrp config** command is used to show the VRRP configuration.

Format

- **show ip vrrp config**

Description

None

Default Value

None

View

Common user view, privileged user view, global configuration view, and VLANIF configuration view

Usage Guidelines

None

Example

Show the VRRP configuration.

```
switch#show ip vrrp config

!vrrp configuration
 ip vrrp enable
 interface vlan 1
 interface vlan 10
 ip vrrp 1
 ip vrrp 1 priority 10
 ip vrrp 1 associate-address 1.1.1.2
 ip vrrp 1 enable
 interface vlan 19
switch#
```

7.8.25 show ip vrrp interface vlan

Function

The **show ip vrrp interface vlan** command is used to show details about a VRRP router (applicable to IPv4).

Format

- **show ip vrrp interface vlan** *vlan-id virtual-route-id*

Parameters

Parameters	Description	Value
virtual-route-id	Specifies the global ID of a virtual router.	The value is an integer in the range from 1 to 255.
vlan-id	Specifies a VLAN ID.	The value is an integer in the range from 1 to 4094.

Default Value

None

View

Common user view, privileged user view, global configuration view, and VLANIF configuration view

Usage Guidelines

None

Example

Show details about a virtual VRRP router.

```
switch#show ip vrrp interface vlan 100 1
  VRRP State:Master,    Virtual Router Id:1
  PriorityRun:100
  PriorityConfig:100
  Preempt:enable
  Virtual Router MAC Address:00:00:5e:00:01:01
  Authentication Mode:none
  Authentication Key:N/A
  Master IP Address:10.0.100.254
  Interface IP Address:10.0.100.254
  Advertisement Interval:10,    Associate IP Address Count:1
  Associated IP Address:10.0.100.1
  BFD-session state:DOWN

  Statistic of this VRRP entry:
  Master Transitions                    : 2
  Received Advertise                    : 0
  Send Priority Zero Packets            : 0
  Received Priority Zero Packets        : 0
  Packet Length Errors                  : 0
  Received Invalid Type Packet          : 0
  Adveritse Interval Errors             : 0
```

```
  IP TTL Errors                    : 0
  Address List Errors              : 0
  New Master Reason                : 4
  Protocol Errors Reason           : 0
  Discontinuity time               : 0
  Refresh Rate                     : 0
  Gratuitous Arp                   : disbale
  Gratuitous Arp Timeout           : 300
  Check TTL                        : disable
switch#
```

7.8.26 show ip vrrp statistic

Function

The **show ip vrrp statistic** command is used to show the statistics of the current VRRP.

Format

- **show ip vrrp statistic**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, and VLANIF configuration view

Usage Guidelines

None

Example

Show the statistics of the current VRRP.

```
switch#show ip vrrp statistic
 vrrp global statistic information:
 Delete Ipv4 Address Count:0
 Delete Ipv4 Address Error Count:0
Add Ipv4 Address Count:0
 Add Ipv4 Address Error Count:0
Delete Virtual Mac Count:0
 Delete Virtual Mac Error Count:0
 Add Virtual Mac Count:0
```

```
 Add Virtual Mac Error Count:0
switch#
```

8. Device Management Commands

8.1 Overview

This chapter introduces the management configuration commands of the N-series switch.

8.2 Hardware Configuration Commands

8.2.1 cpu low-threshold

Function

The **cpu low-threshold** command is used to set the lower limit of CPU usage.

Format

- **cpu** { *slot-number/card-number/cpu-number* | **all** } **low-threshold** *low-threshold*

Parameters

Parameters	Description	Value
slot-number	Specifies the card slot number.	The value is an integer such as 1.
card-number	Specifies the card number.	The value is an integer such as 0
cpu-number	Specifies the CPU number.	The value is an integer such as 1
all	Indicates all CPUs.	-
low-threshold	Specifies the lower limit of CPU usage.	The value is an integer in the range from 0 to 100.

Default Value

The default lower limit of CPU usage is 0.

View

Global configuration view

Usage Guidelines

When the CPU usage is below the lower limit, the switch triggers an alarm if the monitoring and alarm reporting are enabled. The default is recommended. If the lower limit is too high, the system frequently reports alarms. If the lower limit is too low, you cannot learn the CPU usage in a timely manner.

Example

Set the lower limit of all CPU usages to 50.

```
switch(config)#cpu all low-threshold 50
```

```
switch(config)#
```

8.2.2 cpu monitor

Function

The **cpu monitor** command is used to enable or disable CPU monitoring.

Format

- **cpu monitor** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables CPU monitoring.	-
disable	Disables CPU monitoring.	-

Default Value

By default, CPU monitoring is enabled.

View

Global configuration view

Usage Guidelines

None

Example

Disable CPU monitoring.

```
switch(config)#cpu monitor disable
switch(config)#
```

8.2.3 cpu trap

Function

The **cpu trap** command is used to enable or disable CPU alarm reporting.

Format

- **cpu** { *slot-number/card-number/cpu-number* | **all** } **trap** { **enable** | **disable** }

Parameters

Parameters	Description	Value
slot-number	Specifies the card slot number.	The value is an integer such as 1.
card-number	Specifies the card number.	The value is an integer such as 0.
cpu-number	Specifies the CPU number.	The value is an integer such as 1.
all	Indicates all CPUs.	-
enable	Enables CPU alarm reporting.	-
disable	Disables CPU alarm reporting.	-

Default Value

By default, CPU alarm reporting is enabled.

View

Global configuration view

Usage Guidelines

None

Example

Enable CPU alarm reporting.

```
switch(config)#cpu all trap enable
switch(config)#
```

8.2.4 fan monitor

Function

The **fan monitor** command is used to enable or disable fan monitoring.

Format

- **fan monitor** { **enable | disable** }

Parameters

Parameters	Description	Value
enable	Enables fan monitoring.	-
disable	Disables fan monitoring.	-

Default Value

By default, fan monitoring is enabled.

View

Global configuration view

Usage Guidelines

None

Example

Disable fan monitoring.

```
switch(config)#fan monitor disable
switch(config)#
```

8.2.5 fan threshold

Function

The **fan threshold** command is used to set the fan speed threshold of a switch.

Format

- **fan** { *fan-number* | **all** } **threshold** *low-threshold high-threshold*

Parameters

Parameters	Description	Value
fan-number	Specifies a fan number.	The value is an integer in the range from 1-1 to 1-3.
all	Indicates all fans.	-
low-threshold	Specifies the lower threshold of fan speed.	The value is an integer in the range from 200 to 5000.
high-threshold	Specifies the upper threshold of fan speed.	The value is an integer in the range from 5000 to 15000.

Default Value

By default, the lower threshold of fan speed is set to 200 for a switch, and the upper threshold 15000.

View

Global configuration view

Usage Guidelines

When the speed of a fan is higher than the upper threshold or is lower than the lower threshold, the switch triggers an alarm if the monitoring and alarm reporting are enabled. The default is recommended.

Example

Set the lower threshold of fan speed to 500 for a switch and upper threshold to 10000.

```
switch(config)#fan all threshold 500 10000
switch(config)#
```

8.2.6 fan all level

Function

The **fan all level** command is used to set the fan speed level of a switch.

Format

- **fan all level** *level-value*

Parameters

Parameters	Description	Value
level-value	Sets the fan speed level of a switch.	The value is an integer in the range from 1 to 10.

Default Value

The default fan speed level of a switch is 4.

View

Global configuration view

Usage Guidelines

None

Example

Set the fan speed level of a switch to 3.

```
switch(config)#fan all level 3
switch(config)#
```

8.2.7 fan all mode

Function

The **fan all mode** command is used to set the fan mode of a switch.

Format

- **fan all mode** { **fixed-speed** | **temperature-control** }

Parameters

Parameters	Description	Value
fixed-speed	Indicates the fixed speed.	-
temperature-control	Indicates the temperature control.	-

Default Value

temperature-control

View

Global configuration view

Usage Guidelines

None

Example

Set the fan mode of a switch to fixed speed.

```
switch(config)#fan all mode fixed-speed
switch(config)#
```

8.2.8 memory high-threshold

Function

The **memory high-threshold** command is used to set the upper limit of memory usage.

Format

- **memory** { *memory-pool-number* | **all** } **high-threshold** *high-threshold*

Parameters

Parameters	Description	Value
memory-pool-number	Specifies the slot number of a service card.	The value is an integer such as <1-1>/<0-0>/<1-1>.
all	Indicates all memory pools.	-
high-threshold	Specifies the upper limit of memory usage.	The value is an integer in the range from 1 to 100.

Default Value

By default, the upper limit of memory usage is 90.

View

Global configuration view

Usage Guidelines

When the memory usage exceeds the upper limit, a switch triggers an alarm if monitoring and alarm reporting are enabled. The default is recommended.

Example

Set the upper limit of memory usage to 70.

```
switch(config)#memory all high-threshold 70
switch(config)#
```

8.2.9 memory low-threshold

Function

The **memory low-threshold** command is used to set the lower limit of memory usage.

Format

- **memory** { *memory-pool-number* | **all** } **low-threshold** *low-threshold*

Parameters

Parameters	Description	Value
memory-pool-number	Specifies the slot number of a service card.	The value is an integer such as <1-1>/<0-0>/<1-1>.
all	Indicates all memory pools.	-
low-threshold	Specifies the lower limit of memory usage.	The value is an integer in the range from 0 to 100.

Default Value

By default, the lower limit of memory usage is 1.

View

Global configuration view

Usage Guidelines

When the memory usage is below the lower limit, a switch triggers an alarm if monitoring and alarm reporting are enabled. The default is recommended.

Example

Set the lower limit of memory usage to 50.

```
switch(config)#memory all low-threshold 50
switch(config)#
```

8.2.10 memory monitor

Function

The **memory monitor** command is used to enable or disable memory monitoring.

Format

- **memory monitor** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables memory monitoring.	-
disable	Disables memory monitoring.	-

Default Value

By default, memory monitoring is enabled.

View

Global configuration view

Usage Guidelines

None

Example

Disable memory monitoring.

```
switch(config)#memory monitor disable
switch(config)#
```

8.2.11memory trap

Function

The **memory trap** command is used to enable or disable memory alarm reporting.

Format

- **memory** { *memory-pool-number* | **all** } **trap** { **enable** | **disable** }

Parameters

Parameters	Description	Value
memory-pool-number	Specifies the slot number of a service card.	The value is an integer such as <1-1>/<0-0>/<1-1>.

Parameters	Description	Value
all	Indicates all memory pools.	-
enable	Enables memory alarm reporting.	-
disable	Disables memory alarm reporting.	-

Default Value

By default, memory alarm reporting is enabled.

View

Global configuration view

Usage Guidelines

This command is used together with the **memory monitor** command.

Example

Disable memory alarm reporting.

```
switch(config)#memory all trap disable
switch(config)#
```

8.2.12 show cpu statistic

Function

The **show cpu statistic** command is used to show CPU usage statistics.

Format

- **show cpu statistic**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Show CPU usage statistics.

```
switch(config)#show cpu statistic
CPU statistics information:
 CPU monitor: enable
 CPU index: Cpu-1/0/1
  CPU current usage: 1.20%
  CPU utilization last-5sec: 1.20%, last-1min: 0.96%, last-5min :0.92%
  Max CPU usage: 20.40%
  Max CPU usage stat time: 10/16/2019 9:06:51 AM
  State: normal
  High threshold: 40%, Low threshold : 0%

 ServiceName              UseRate
 (tNLMSG)                  0.00%
 (fspdriver)              0.00%
 (tIfLinkTask)            0.00%
 (tVlanAutoTask)          0.00%
 (tArlTask)               0.00%
 (tIfAppTask)             0.00%
 (tMVRX)                   0.00%
 (tBFDL)                  0.00%
 (tMNTR)                   0.00%
 (tSYNC)                  0.00%
 (tAntiArp)               0.00%
 (fspsysmonitor)          0.19%
 (fspflush)               0.00%
 (fspmam)                  0.00%
 (fspmirror)              0.00%
 (fsptimerange)           0.00%
 (fspddm)                  0.00%
 (fspportisolate)         0.00%
 (fspacl)                 0.00%
 (fspcpudefend)           0.00%
 (fsppoe)                  0.19%
 (fspmendxlatevla)        0.00%
 (fspvlanmapping)         0.00%
 (fspqinq)                0.00%
 (fspaaa)                 0.00%
 (fspdot1x)               0.00%
```

(fspmstp) 0.00%
(fspg8032) 0.00%
(fspflink) 0.00%
(fspmlink) 0.00%
(fspalb) 0.00%
(fspscheduleprof) 0.00%
(fsplacp) 0.00%
(fsphwmc) 0.00%
(fspigmpsnoop) 0.00%
(fspmldsnoop) 0.00%
(fspbpdutunnel) 0.00%
(fsplinkflap) 0.00%
(fspstormsuppr) 0.00%
(fspstormctrl) 0.00%
(fspvtp) 0.00%
(fsplldp) 0.19%
(fspudld) 0.00%
(fspmvrp) 0.00%
(fspdot1ag) 0.00%
(fspy1731) 0.00%
(fspdot3ah) 0.00%
(fspbfd) 0.00%
(fspnqa) 0.00%
(fsppppoeplus) 0.00%
(fsparpprobe) 0.00%
(fsphwroutefrr) 0.00%
(fspl3vpn) 0.00%
(fspntp) 0.00%
(fsproutepolicy) 0.00%
(fspipprefix) 0.00%
(fspaspath) 0.00%
(fspospfv2) 0.00%
(fspisis) 0.00%
(fspbgp) 0.00%
(fsprip) 0.00%
(fspospfv3) 0.00%
(fspripng) 0.00%
(fspigmp) 0.00%
(fsppim) 0.00%
(fspmld) 0.00%
(fsppim6) 0.00%

```
(fspsmartinstall)     0.00%
(fspdhcp)             0.00%
(fspdhcp6)            0.00%
(fspipsg)             0.00%
(fspdhcpsnoop)        0.00%
(fspdhcpc)            0.00%
(fspvrrp)             0.00%
(fspiss)              0.00%
(fspmad)              0.00%
(fspvoicevlan)        0.00%
(fspdevice)           0.39%
(fspnmagent)          0.19%
(tMSGQ)               0.00%
switch(config)#
```

8.2.13 show fan

Function

The **show fan** command is used to show the fan state.

Format

- **show fan**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Show the fan state.

```
switch(config)#show fan
Fan information:
 Fan monitor: enable
   FanCtrl        Speed    Level    L-Threshold H-Threshold Status        Trap     Mode          Serial
Descr
```

```
*  Fan-1/1    8600  4  200  15000  normal  enable  temperature-ctrl  N/A
CTRL-1/1
*  Fan-1/2    8200  4  200  15000  normal  enable  temperature-ctrl  N/A
CTRL-1/2
*  Fan-1/3    8500  4  200  15000  normal  enable  temperature-ctrl  N/A
CTRL-1/3
*  Fan-1/4    8400  4  200  15000  normal  enable  temperature-ctrl  N/A
CTRL-1/4
*  Fan-1/5    8400  4  200  15000  normal  enable  temperature-ctrl  N/A
CTRL-1/5
*  Fan-1/6    8500  4  200  15000  normal  enable  temperature-ctrl  N/A
CTRL-1/6

switch(config)#
```

8.2.14 show memory pool

Function

The **show memory pool** command is used to show memory pool usage of all current switches.

Format

- **show memory pool**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Show memory pool usage of switches.

```
switch(config)#show memory pool
Memory pool information:
 Memory pool monitor: enable
 Memory pool: Memory-1/0/1
  Total memory        : 512984 KB
```

```
Total memory used: 163048 KB
Current usage      : 31.97%
Max usage          : 31.97%
Trap state         : enable
Status             : normal
High threshold     : 90%, Low threshold : 1%

ServiceName            MemUsage(Kb)
init                   628
init.sh                624
fspdriver              23092
fspsysmonitor          1468
fspflush               1140
fspmam                 16248
fspmirror              1160
fsptimerange           1372
fspddm                 1268
fspportisolate         3492
fspacl                 6852
fspcpudefend           1364
fsppoe                 1252
fspmendxlatevla        11904
fspvlanmapping         1892
fspqinq                1436
fspaaa                 1200
fspdot1x               1640
fspmstp                6804
fspg8032               1180
fspflink               1324
fspmlink               1252
fspalb                 1220
fspscheduleprof        1184
fsplacp                1272
fsphwmc                1292
fspigmpsnoop           1484
fspmldsnoop            1124
fspbpdutunnel          2988
fsplinkflap            1156
fspstormsuppr          1256
fspstormctrl           2388
fspvtp                 1428
```

```
fsplldp                 1488
fspudld                 1180
fspmvrp                 2124
fspdot1ag               1232
fspy1731                1244
fspdot3ah               1176
fspbfd                  1336
fspnqa                  1156
fsppppoeplus            1244
fsparpprobe             1504
fsphwroutefrr           8600
fspl3vpn                1496
fspntp                  1252
fsproutepolicy          1660
fspipprefix             1272
fspaspath               1276
fspospfv2               1280
fspisis                 1264
fspbgp                  1848
fsprip                  1356
fspospfv3               1344
fspripng                1236
fspigmp                 1228
fsppim                  1168
fspmld                  1244
fsppim6                 1172
fspsmartinstall         1240
fspdhcp                 1240
fspdhcp6                1228
fspipsg                 1188
fspdhcpsnoop            1548
fspdhcpc                1672
fspvrrp                 2012
fspiss                  1304
fspmad                  1192
fspvoicevlan            1172
fspdevice               1400
fspnmagent              30420
switch(config)#
```

8.2.15 show temperature

Function

The **show temperature** command is used to show the temperature of a switch.

Format

- **show temperature**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Show the temperature of a switch.

```
switch#show temperature
Temperature information:
 Temperature monitor: enable
    Index                CurrValue L-Threshold H-Threshold RE-L-Threshold RE-H-Threshold RE-State      Status    Trap
Descr
*   Temper-1/0/1    41           -10          68           -30          90           disable      normal    enable
Sensor Temperature
switch#
```

8.2.16 show temperature config

Function

The **show temperature config** command is used to show the temperature configuration of a switch.

Format

- **show temperature config**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Show the temperature configuration of a switch.

```
switch(config)#show temperature config
 temperature 1/0/1 threshold 30 60
switch(config)#
```

8.2.17 temperature monitor

Function

The **temperature monitor** command is used to enable or disable temperature monitoring.

Format

- **temperature monitor** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables temperature monitoring.	-
disable	Disables temperature monitoring.	-

Default Value

By default, temperature monitoring is enabled.

View

Global configuration view

Usage Guidelines

Generally, this command is used together with the temperature trapcommand to monitor the switch temperature.

Example

Disable temperature monitoring.

```
switch(config)#temperature monitor disable
switch(config)#
```

8.2.18 temperature threshold

Function

The **temperature threshold** command is used to set temperature threshold for a switch.

Format

- **temperature** { *temperature-number* | **all** } **threshold** *low-threshold high-threshold*

Parameters

Parameters	Description	Value
temperature-number	Specifies the temperature number.	The value is an integer such as <1-1>/<0-0>/<1-1>.
all	Indicates all temperature.	-
low-threshold	Specifies the lower temperature threshold.	The value is an integer in the range from -60 to 30.
high-threshold	Specifies the upper temperature threshold.	The value is an integer in the range from 30 to 150.

Default Value

By default, the lower threshold of temperature is set to 0 for a switch, and the upper threshold 75.

View

Global configuration view

Usage Guidelines

When the temperature is higher than the upper threshold or is lower than the lower threshold, a switch triggers an alarm if monitoring and reporting alarms are enabled. The default is recommended.

Example

Set the lower temperature threshold for a switch to 20 and upper threshold to 58.

```
switch(config)#temperature all threshold 20 58
switch(config)#
```

8.2.19 temperature trap

Function

The **temperature trap** command is used to enable or disable temperature alarm reporting.

Format

- **temperature** { *temperature-number* | **all** } **trap** { **enable** | **disable** }

Parameters

Parameters	Description	Value
temperature-number	Specifies the temperature number.	The value is an integer such as <1-1>/<0-0>/<1-1>.
all	Indicates all temperature.	-
enable	Enables temperature alarm reporting.	-
disable	Disables temperature alarm reporting.	-

Default Value

By default, temperature alarm reporting is enabled.

View

Global configuration view

Usage Guidelines

None

Example

Disable temperature alarm reporting.

```
switch(config)#temperature all trap disable
switch(config)#
```

8.3 Mirror Configuration Commands

8.3.1 mirror group (Local Mirror)

Function

The **mirror group** command is used to configure a local mirror group and its observing port.
The **no mirror group** command is used to delete a local mirror group and its observing port.

Format

- **mirror group** *group-num* { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **no mirror group** [*group-num*]

Description

Parameters	Description	Value
group-num	Specifies a mirror group ID.	The value is an integer in the range from 1 to 7.
interface-number	Specifies the number of the Ethernet interface acting as an observing port.	The value is an integer in the range of <1-1>/<0-2>/<1-52>.

Default Value

By default, no local observing group or its observing port is configured.

View

Global configuration view

Usage Guidelines

When an observing port and observed port (source port of mirroring) are on the same switch, you can use this command to configure a local mirror group and its observing port.
If an interface is designated as an observing port, do not perform other configurations on this interface. Otherwise, the mirror function may be affected.
To change a local observing port to a remote observing port, you must delete the original configuration and then configure the port again.

Example

Configure a local mirror group and specify 10gigaethernet 1/0/1 as its observing port.

```
switch(config)#mirror group 1 10gigaethernet 1/0/1
switch(config)#
```

Warning: The maximum number of mirror group is up to two.

8.3.2 show mirror config

Function

The **show mirror config** command is used to show the mirroring configuration on a switch.

Format

- **show mirror config**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), VLAN configuration view, and interface group configuration view

Usage Guidelines

This command does not show L2, L3, and local mirroring information simultaneously. The initialized information is 0.

Example

Show the mirroring configuration.

```
switch#show mirror config
Version : MIRROR_VX2.10.00.00
 mirror group 1 10gigaethernet 1/0/1
interface 10ge-1/0/5
 mirror ingress group 1
switch#
```

8.3.3 show mirror group

Function

The **show mirror group** command is used to show mirror group information on a switch.

Format

- **show mirror group**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), VLAN configuration view, and interface group configuration view

Usage Guidelines

This command does not show L2, L3, and local mirroring information simultaneously. The initialized information is 0.

Example

Show mirror group information.

```
switch#show mirror group
 Mirror group 1 is set to 10 interface ge-1/0/1
```

```
 Mirror group type: Local
switch#
```

8.3.4 show mirror interface

Function

The **show mirror interface** command is used to show the interface mirroring usage on a switch.

Format

- **show mirror interface**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), VLAN configuration view, and interface group configuration view

Usage Guidelines

None

Example

Show the interface mirroring usage.

```
switch#show mirror interface
  Interface    Mac-address/Mask    Mirror-group    Direction
 10ge-1/0/5          ----                1            ingress
switch#
```

8.4 NTP Configuration Commands

8.4.1 debug ntp

Function

The **debug ntp** command enables ntp debugging.
The **no debug ntp** command disables ntp debugging.

Format

- **debug ntp { error | pkt | warning | event | auth | all }**
- **no debug ntp { error | pkt | warning | event | auth | all }**

Parameters

Parameter	Description	Value
error	Enable debugging of error information.	-
pkt	Enable debugging of packet information.	-
warning	Enable debugging of warning information.	-
event	Enable debugging of event information.	-
auth	Enable debugging of MD5 authentication information.	-
all	Enable debugging of all information.	-

Default Value

By default, The NTP debugging is disabled.

View

privileged user view

Usage Guidelines

Use this command to view the NTP protocol process and the status of sending and receiving packets. This command is used to maintain and debug the NTP function of the device.

Example

Enable NTP debugging.

```
switch#debug ntp all
switch#
```

Disable NTP debugging.

```
switch#no debug ntp all
switch#
```

8.4.2 ntp

Function

The **ntp** command enables the system to display the NTP configuration view.

Format

ntp

Parameters

None

Default Value

None

View

global configuration view

Usage Guidelines

This command is a prerequisite for configuring other NTP parameters.

Example

Enter the configuration view of NTP from global configuration view.

```
switch(config)#ntp
switch(config-ntp)#
```

8.4.3 ntp broadcast-client

Function

The **ntp broadcast-client**command configures the device to work in NTP broadcast client mode.
The **no ntp broadcast-client** command removes the device from the NTP broadcast client mode.

Format

- **ntp broadcast-client**
- **ntp broadcast-client ipv4-address**
- **no ntp broadcast-client**
- **no ntp broadcast-client ipv4-address**

Parameters

Parameters	Description	Value
ipv4-address	Specifies the broadcast IP address	The default value is 255.255.255.0

Default Value

The default value is 255.255.255.0

View

VLANIF configuration view、Ethernet routing interface configuration view、grp route interface configuration view

Usage Guidelines

On a synchronization sub-net, when the IP address of a server or a symmetric peer is not determined, or when the clocks on a large number of devices need to be synchronized on the network, you can implement clock synchronization by configuring the broadcast mode.

Example

Enable ntp broadcast-client mode.

```
switch(config-vlanif-4002)#ntp broadcast-client
```

```
switch(config-vlanif-4002)#
```

8.4.4 ntp multicast-client

Function

The **ntp multicast-client** command configures the local device to work in NTP multicast client mode.
The **no ntp multicast-client** command cancels the NTP multicast client mode.

Format

- **ntp multicast-client**
- **ntp multicast-client ipv4-address**
- **no ntp multicast-client ipv4-address**
- **no ntp multicast-client**

Parameters

Parameters	Description	Value
ipv4-address	multicast IP address	The value is in dotted decimal notation.The default value is 224.0.1.1.

Default Value

multicast IP address, The default value is 224.0.1.1

View

VLANIF configuration view 、Ethernet routing interface configuration view、grp route interface configuration view

Usage Guidelines

Indicates the multicast IP address.

Example

Add the multicast address of the multicast packets is239.255.255.255.

```
switch(config-vlanif-4002)#ntp multicast-client 239.255.255.255
switch(config-vlanif-4002)#
```

8.4.5 ntp broadcast-server

Function

The **ntp broadcast-server** command configures the local device to work in NTP broadcast server mode.
The **no ntp broadcast-server** command removes the device from the NTP broadcast server mode.

Format

- **ntp broadcast-server**
- **ntp broadcast-server ipv4-address**
- **ntp broadcast-server authentication-keyid key-id**

- **ntp broadcast-server authentication-keyid key-id ipv4-address**
- **ntp broadcast-server version { 1 | 2 | 3 | 4 }**
- **ntp broadcast-server version { 1 | 2 | 3 | 4 } ipv4-address**
- **ntp broadcast-server authentication-keyid key-id version { 1 | 2 | 3 | 4 }**
- **ntp broadcast-server authentication-keyid key-id version { 1 | 2 | 3 | 4 } ipv4-address**
- **no ntp broadcast-server**
- **no ntp broadcast-server ipv4-address**

Parameters

Parameters	Description	Value
key-id	Indicates the authentication key number used to transmit a message to broadcast clients.	The value is an integer ranging from 1 to 4294967295.
version { 1 | 2 | 3 | 4 }	Indicates the NTP version number.	The default value is 3.
ipv4-address	Specifies the broadcast IP address	The value is in dotted decimal notation, The default value is 255.255.255.0.

Default Value

The default version number of NTP broadcast-server is 3.

View

VLANIF configuration view, Ethernet routing interface configuration view、grp route interface configuration view

Usage Guidelines

Using this command can be used to specify an interface on local device to send NTP broadcasts, the local running in server mode. As a broadcast server, periodically send broadcast message to the client.

Example

#Enable NTP server with version as 1.

```
switch(config-vlanif-1)#ntp broadcast-server authentication-keyid 1 version 1
switch(config-vlanif-1)#
```

8.4.6 ntp multicast-server

Function

The **ntp multicast-server** command configures the local device to work in NTP multicast server mode.
The **no ntp multicast-server** command removes the device from the NTP multicast server mode.

Format

- **ntp multicast-server**
- **ntp multicast-server ipv4-address**

- **ntp multicast-server authentication-keyid key-id**
- **ntp multicast-server authentication-keyid key-id ipv4-address**
- **ntp multicast-server version { 1 | 2 | 3 | 4 }**
- **ntp multicast-server version { 1 | 2 | 3 | 4 } ipv4-address**
- **ntp multicast-server ttl ttl-value**
- **ntp multicast-server ttl ttl-value ipv4-address**
- **ntp multicast-server version { 1 | 2 | 3 | 4 } ttl ttl-value**
- **ntp multicast-server version { 1 | 2 | 3 | 4 } ttl ttl-value ipv4-address**
- **ntp multicast-server authentication-keyid key-id version { 1 | 2 | 3 | 4 } ttl ttl-value**
- **ntp multicast-server authentication-keyid key-id version { 1 | 2 | 3 | 4 } ttl ttl-value ipv4-address**
- **no ntp multicast-server**
- **no ntp multicast-server ipv4-address**

Parameters

Parameters	Description	Value
Key-id	Indicates the authentication key ID used when sending messages to the multicast clients.	The value is an integer ranging from 1 to 4294967295.
ipv4-address	Multicast IPV4 address	The value is in dotted decimal notation.
version { 1 | 2 | 3 | 4 }	Indicates the NTP version number.	The default value is 3.
ttl-value	Indicates the life span of the multicast packet.	The value is an integer ranging from 1 to 255.The default value is 8.

Default Value

multicast IP address, The default value is 224.0.1.1

View

VLANIF configuration view、Ethernet routing interface configuration view、grp route interface configuration view

Usage Guidelines

The required IP address must be a multicast IP.

Example

Enable NTP multicast server.

```
switch(config-vlanif-4002)#ntp multicast-server version 2 ttl 254
switch(config-vlanif-4002)#
```

8.4.7 show ntp

Function

The **show ntp** command is used to show the NTP global configuration information.

Format

show ntp

Parameters

None

Default Value

None

View

Configuration view

Usage Guidelines

Using this command, the NTP configuration information is given in the form of a configuration file, and the user can check whether the NTP global configuration information correct.

Example

Show the NTP global configuration information.

```
switch#show ntp
 Version                          : NTP_VB3.00.00.00
 ntp once sync                    : disable
 ntp client update-interval       : 64s
 ntp server broadcast-interval     : 64s
 ntp stratum                      : 16
 ntp master                       : false
 ntp authentication               : disable
switch#
```

8.4.8 show ntp service

Function

The **show ntp service** command displays the service of NTP.

Format

show ntp service

Parameters

None

Default Value

None

View

Common user view

Usage Guidelines

None

Example

displays the information of NTP Configuration.

```
switch#show ntp service
Mode              Source       Version key-id      Offset(s)     Delay(s)              Disper(s)
unicast-peer      ::           2       2       0.000000        0.000000                16.000000
unicast-peer 192.168.2.202 3 4294927694 0.000000     0.000000                16.000000
unicast-client    ::         1         1             0.000000          0.000000            16.000000
unicast-client   192.168.1.202   4 4294927695 0.000000   0.000000                16.000000
switch#
```

8.4.9 show ntp service verbose

Function

The **show ntp service verbose** command displays the verbose of NTP service.

Format

- **show ntp service verbose**

Parameters

None

Default Value

None

View

Common user view

Usage Guidelines

None

Example

displays the verbose of NTP service.

```
switch#show ntp service verbose
clock source: ::
 clock stratum: 16
 reference clock ID: ::
 local mode: active, local poll: 4
 peer mode: passive, peer poll: 0
 offset: 0.000000s, delay: 0.000000s, disper: 16.000000s
 root delay: 0.000000s, root disper: 0.000000s
precision: -18, version: 2
 reftime: 00:00:00 UTC Jan 00 1900 (0.0)
 orgtime: 00:00:00 UTC Jan 00 1900 (0.0)
 rcvtime: 00:00:00 UTC Jan 00 1900 (0.0)
 xmttime: 00:00:00 UTC Jan 00 1900 (0.0)

 clock source: 192.168.2.202
 clock stratum: 16
 reference clock ID: 192.168.2.202
 local mode: active, local poll: 4
 peer mode: passive, peer poll: 0
 offset: 0.000000s, delay: 0.000000s, disper: 16.000000s
 root delay: 0.000000s, root disper: 0.000000s
 precision: -18, version: 3
 reftime: 00:00:00 UTC Jan 00 1900 (0.0)
 orgtime: 00:00:00 UTC Jan 00 1900 (0.0)
 rcvtime: 00:00:00 UTC Jan 00 1900 (0.0)
 xmttime: 04:54:21 UTC Nov 01 2006 (c8f2a6fd.2666664c)

 clock source: ::
 clock stratum: 16
 reference clock ID: ::
 local mode: client, local poll: 4
 peer mode: server, peer poll: 0
 offset: 0.000000s, delay: 0.000000s, disper: 16.000000s
 root delay: 0.000000s, root disper: 0.000000s
 precision: -18, version: 1
 reftime: 00:00:00 UTC Jan 00 1900 (0.0)
 orgtime: 00:00:00 UTC Jan 00 1900 (0.0)
 rcvtime: 00:00:00 UTC Jan 00 1900 (0.0)
 xmttime: 00:00:00 UTC Jan 00 1900 (0.0)
```

clock source: 192.168.1.202
clock stratum: 16
reference clock ID: 192.168.1.202
local mode: client, local poll: 4
peer mode: server, peer poll: 0
offset: 0.000000s, delay: 0.000000s, disper: 16.000000s
root delay: 0.000000s, root disper: 0.000000s
precision: -18, version: 4
reftime: 00:00:00 UTC Jan 00 1900 (0.0)
orgtime: 00:00:00 UTC Jan 00 1900 (0.0)
rcvtime: 00:00:00 UTC Jan 00 1900 (0.0)
xmttime: 04:54:22 UTC Nov 01 2006 (c8f2a6fe.2666664c)

clock source: ::
clock stratum: 16
reference clock ID: ::
local mode: server, local poll: 5
peer mode: client, peer poll: 0
offset: 0.000000s, delay: 0.000000s, disper: 16.000000s
root delay: 0.000000s, root disper: 0.000000s
precision: -18, version: 1
reftime: 00:00:00 UTC Jan 00 1900 (0.0)
orgtime: 00:00:00 UTC Jan 00 1900 (0.0)
rcvtime: 00:00:00 UTC Jan 00 1900 (0.0)
xmttime: 04:54:19 UTC Nov 01 2006 (c8f2a6fb.2666664c)

clock source: 0.0.0.0
clock stratum: 16
reference clock ID: 0.0.0.0
local mode: server, local poll: 5
peer mode: client, peer poll: 0
offset: 0.000000s, delay: 0.000000s, disper: 16.000000s
root delay: 0.000000s, root disper: 0.000000s
precision: -18, version: 4
reftime: 00:00:00 UTC Jan 00 1900 (0.0)
orgtime: 00:00:00 UTC Jan 00 1900 (0.0)
rcvtime: 00:00:00 UTC Jan 00 1900 (0.0)
xmttime: 04:54:19 UTC Nov 01 2006 (c8f2a6fb.2666664c)

clock source: 0.0.0.0

```
 clock stratum: 16
 reference clock ID: 0.0.0.0
 local mode: server, local poll: 5
 peer mode: client, peer poll: 0
 offset: 0.000000s, delay: 0.000000s, disper: 16.000000s
 root delay: 0.000000s, root disper: 0.000000s
 precision: -18, version: 4
 reftime: 00:00:00 UTC Jan 00 1900 (0.0)
 orgtime: 00:00:00 UTC Jan 00 1900 (0.0)
 rcvtime: 00:00:00 UTC Jan 00 1900 (0.0)
 xmttime: 04:54:19 UTC Nov 01 2006 (c8f2a6fb.2666664c)
switch#
```

8.4.10 show ntp config

Function

The **show ntp config** command displays the NTP configuration information.

Format

show ntp config

Parameters

None

Default Value

None

View

Common user view

Usage Guidelines

None

Example

Display NTP configuration information.

```
switch#show ntp config
!
ntp
 client update-interval 10
 stratum 9
 authentication enable
 ntp unicast-peer 201.1.1.1 version 4
```

```
switch#
```

8.4.11authentication {enable|disable}

Function

The **authentication {enable|disable}** command enables or disables identity authentication for MD5.

Format

- **authentication { enable | disable }**

Parameters

Parameters	Description	Value
enable	Enable MD5 authentication	-
disable	Disable MD5 authentication	-

Default Value

By default, disables identity authentication for MD5.

View

NTP configuration view

Usage Guidelines

Use this command to enable MD5 authentication globally. MD5 authentication can be used for networks with higher security.

Example

Enable MD5 authentication

```
switch(config-ntp)#authentication enable
switch(config-ntp)#
```

Disable MD5 authentication

```
switch(config-ntp)#authentication disable
switch(config-ntp)#
```

8.4.12 authentication-keyid

Function

The **authentication-keyi**d command configures an NTP authentication keyid**.**
The **no authentication-keyid** command remove the NTP authentication keyid.

Format

- **authentication-keyid** *key-id* **md5 key** *key-string*
- **authentication-keyid key-id md5 key { cipher | plain } key-string**
- **no authentication-keyid key-id**

Parameters

Parameter	Description	Value
key-id	key-id	The value is an integer ranging from 1 to 4294967295.
key-string	key-string	The value is a character string in the range of 1 to 16
{ cipher | plain }	Specifies the authentication password in plain text or in cipher text.	-

Default Value

NTP authentication key is not configured by default.

View

NTP configuration view

Usage Guidelines

Use this command to configure an NTP authentication key and enables the md5 algorithm for authentication

Example

Set the MD5 identity authentication key. Set the key ID number to 100 and the key to FHNtestkey.

```
switch(config-ntp)#authentication-keyid 100 md5 key FHNtestkey
switch(config-ntp)#
```

delete the authentication key

```
switch(config-ntp)#no authentication-keyid 100
switch(config-ntp)#
```

8.4.13 client update-interval

Function

The **client update-interval** command enable the NTP client to update-interval.

Format

- **client update-interval { update-interval-time | default }**

Parameters

Parameters	Description	Value
update-interval-time	Specify NTP client update interval time.	The value is an integer in range from 4 to 17, the power of 2 seconds.
default	The default value of NTP client update interval time.	The value is a character string.

Default Value

The default value of NTP client update interval is 6, which is 2 to the 6th power of seconds.

View

NTP configuration view

Usage Guidelines

the power of 2 seconds.

Example

Configure the NTP client interval time as 8, which is 2 to the 8th power of seconds.

```
switch(config-ntp)# client update-interval 8
switch(config-ntp)#show ntp
 ntp client update-interval      : 256s
 ntp server broadcast-interval : 64s
 ntp stratum                          : 16
 ntp master                           : false
 ntp authentication                 : disable
switch(config-ntp)#
```

8.4.14 ntp unicast-peer

Function

The **ntp unicast-peer** command configures IPv4 NTP peer mode.
The **o ntp unicast-peer** command cancels the IPv4 NTP peer mode.

Format

- **ntp unicast-peer ipv4-address**
- **ntp unicast-peer ipv4-address authentication-keyid** *key-id*
- **ntp unicast-peer ipv4-address authentication-keyid** *key-id* **source-interface loopback** *loopback-number*
- **ntp unicast-peer ipv4-address authentication-keyid** *key-id* **source-interface vlan** *vlan-id*
- **ntp unicast-peer ipv4-address authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name*
- **ntp unicast-peer ipv4-address authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name* **source-interface loopback** *loopback-number*

- **ntp unicast-peer ipv4-address authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name* **source-interface vlan** *vlan-id*
- **ntp unicast-peer ipv4-address authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name* **source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **ntp unicast-peer ipv4-address authentication-keyid** *key-id* **source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **ntp unicast-peer ipv4-address source-interface loopback** *loopback-number*
- **ntp unicast-peer ipv4-address source-interface vlan** *vlan-id*
- **ntp unicast-peer ipv4-address source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **ntp unicast-peer ipv4-address version** *version-value*
- **ntp unicast-peer ipv4-address version** *version-value* **authentication-keyid** *key-id*
- **ntp unicast-peer ipv4-address version** *version-value* **authentication-keyid** *key-id* **source-interface loopback** *loopback-number*
- **ntp unicast-peer ipv4-address version** *version-value* **authentication-keyid** *key-id* **source-interface vlan** *vlan-id*
- **ntp unicast-peer ipv4-address version** *version-value* **authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name*
- **ntp unicast-peer ipv4-address version** *version-value* **authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name* **source-interface loopback** *loopback-number*
- **ntp unicast-peer ipv4-address version** *version-value* **authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name* **source-interface vlan** *vlan-id*
- **ntp unicast-peer ipv4-address version** *version-value* **authentication-keyid** *key-id* **source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **ntp unicast-peer ipv4-address version** *version-value* **authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name* **source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **ntp unicast-peer ipv4-address version** *version-value* **source-interface loopback** *loopback-number*
- **ntp unicast-peer ipv4-address version** *version-value* **source-interface vlan** *vlan-id*
- **ntp unicast-peer ipv4-address version** *version-value* **source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **ntp unicast-peer ipv4-address version version-value vpn-instance vpn-instance-name**
- **ntp unicast-peer ipv4-address version** *version-value* **vpn-instance** *vpn-instance-name* **source-interface loopback** *loopback-number*
- **ntp unicast-peer ipv4-address version** *version-value* **vpn-instance** *vpn-instance-name* **source-interface vlan** *vlan-id*
- **ntp unicast-peer ipv4-address version** *version-value* **vpn-instance** *vpn-instance-name* **source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **ntp unicast-peer ipv4-address vpn-instance** *vpn-instance-name*
- **ntp unicast-peer ipv4-address vpn-instance** *vpn-instance-name* **source-interface loopback** *loopback-number*
- **ntp unicast-peer ipv4-address vpn-instance** *vpn-instance-name* **source-interface vlan** *vlan-id*
- **ntp unicast-peer ipv4-address vpn-instance** *vpn-instance-name* **source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **no ntp unicast-peer ipv4-address**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IP address	The value is in dotted decimal notation

Parameter	Description	Value
version-value	Specifies version-value	The value is an integer ranging from 1 to 4.
key-id	Specifies the key ID for the NTP authentication.	The value is an integer ranging from 1 to 4294967295.
vpn-instance-name	Specifies vpn-instance-name	The value is a character string,maximum length is 31
loopback-number	Specifies loopback-number	The value is an integer ranging from 1 to 127.
vlan-id	Specifies VLAN ID	The value is an integer ranging from 1 to 4094.
interface-number	Specifies interface-number	The value is an integer ranging from<1-1>/<0-1>/<1-48>.

Default Value

Indicates the NTP version number, The default value is 3

View

NTP configuration view

Usage Guidelines

This command can be used to specify or not specify an IPv4 peer for the device. The specified IP address is the IP address of the peer device, and the version refers to the key configured by the NTP protocol version number.

Example

#Configure a IPv4 NTP unicast-peer.

```
switch(config-ntp)#ntp unicast-peer 1.1.1.1 version 3 authentication-keyid 100
switch(config-ntp)#
```

#Configure a IPv4 NTP unicast-peer with VPN-instace.

```
switch(config-ntp)#ntp unicast-peer 192.168.2.202 version 1 authentication-keyid 4294967295 vpn-instance vpn1
switch(config-ntp)#
```

8.4.15 master

Function

The **master** command sets the local clock to be the NTP primary clock
The **no master** command cancels the configuration of the NTP primary clock.

Format

- **master**
- **no master**

Parameters

None

Default Value

By default, no NTP primary clock is specified.

View

NTP configuration view

Usage Guidelines

This command can be used to specify the device as the master clock. Only the device configured as the master clock can be used as a server on the network to synchronize the time of other devices.

Example

Set the local clock to be the NTP primary clock

```
switch(config-ntp)#master
switch(config-ntp)#
```

8.4.16 ntp unicast-server

Function

The **ntp unicast-server** command configures the NTP server mode.
The **no ntp unicast-server** command cancels the NTP server mode.

Format

- **ntp unicast-server ipv4-address**
- **ntp unicast-server ipv4-address authentication-keyid** *key-id*
- **ntp unicast-server ipv4-address authentication-keyid** *key-id* **source-interface loopback** *loopback-number*
- **ntp unicast-server ipv4-address authentication-keyid** *key-id* **source-interface vlan** *vlan-id*
- **ntp unicast-server ipv4-address authentication-keyid** *key-id* **source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **ntp unicast-server ipv4-address authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name*
- **ntp unicast-server ipv4-address authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name* **source-interface loopback** *loopback-number*
- **ntp unicast-server ipv4-address authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name* **source-interface vlan** *vlan-id*
- **ntp unicast-server ipv4-address authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name* **source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **ntp unicast-server ipv4-address source-interface loopback** *loopback-number*
- **ntp unicast-server ipv4-address source-interface vlan** *vlan-id*
- **ntp unicast-server ipv4-address source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **ntp unicast-server ipv4-address version** *version-value*
- **ntp unicast-server ipv4-address version** *version-value* **authentication-keyid** *key-id*
- **ntp unicast-server ipv4-address version** *version-value* **authentication-keyid** *key-id* **source-interface loopback** *loopback-number*

- **ntp unicast-server ipv4-address version** *version-value* **authentication-keyid** *key-id* **source-interface vlan** *vlan-id*
- **ntp unicast-server ipv4-address version** *version-value* **authentication-keyid** *key-id* **source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **ntp unicast-server ipv4-address version** *version-value* **authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name*
- **ntp unicast-server ipv4-address version** *version-value* **authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name* **source-interface loopback** *loopback-number*
- **ntp unicast-server ipv4-address version** *version-value* **authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name* **source-interface vlan** *vlan-id*
- **ntp unicast-server ipv4-address version** *version-value* **authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name* **source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **ntp unicast-server ipv4-address version** *version-value* **source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **ntp unicast-server ipv4-address version** *version-value* **source-interface loopback** *loopback-number*
- **ntp unicast-server ipv4-address version** *version-value* **source-interface vlan** *vlan-id*
- **ntp unicast-server ipv4-address version** *version-value* **vpn-instance** *vpn-instance-name*
- **ntp unicast-server ipv4-address version** *version-value* **vpn-instance** *vpn-instance-name* **source-interface loopback** *loopback-number*
- **ntp unicast-server ipv4-address version** *version-value* **vpn-instance** *vpn-instance-name* **source-interface vlan** *vlan-id*
- **ntp unicast-server ipv4-address version** *version-value* **vpn-instance** *vpn-instance-name* **source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **ntp unicast-server ipv4-address vpn-instance** *vpn-instance-name*
- **ntp unicast-server ipv4-address vpn-instance** *vpn-instance-name* **source-interface loopback** *loopback-number*
- **ntp unicast-server ipv4-address vpn-instance** *vpn-instance-name* **source-interface vlan** *vlan-id*
- **ntp unicast-server ipv4-address vpn-instance** *vpn-instance-name* **source-interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
- **no ntp unicast-server ipv4-address**

Parameters

Parameters	Description	Value
ipv4-address	Indicates the IPv4 address of the server.	The value is in dotted decimal notation.
version-value	Specifies NTP version-value	The value is an integer ranging from 1 to 4, the default version-value is 3.
key-id	Specifies NTP key-id	The value is an integer ranging from 1 to 4294967295
vpn-instance-name	Specifies vpn-instance-name	The value is a character string, maximum length is 30
loopback-number	Specifies loopback-number	The value is an integer ranging from 1 to127
vlan-id	Specifies VLAN ID	The value is an integer ranging from 1 to 4094
interface-number	Specifies interface-number	The value is an integer ranging from<1-1>/<0-1>/<1-48>

Default Value

NTP version-value, The default value is 3

View

NTP configuration view

Usage Guidelines

None

Example

#Configure IPv4 NTP unicast server.

```
switch(config-ntp)#ntp unicast-server 1.1.1.1 version 4 authentication-keyid 100
switch(config-ntp)#
```

#Configure IPv4 NTP unicast server with vpn-instance.

```
switch(config-ntp)#ntp unicast-server 192.168.1.205 vpn-instance vpn1
switch(config-ntp)#
```

8.4.17 oncesync { enable | disable }

Function

The **oncesync enable** command enables one-time synchronization of message.
The **oncesync disable** command disables one-time synchronization of message.

Format

- **oncesync { enable | disable }**

Parameters

Parameters	Description	Value
enable	enable one-time synchronization	-
disable	disable one-time synchronization	-

Default Value

Disable

View

NTP configuration view

Usage Guidelines

This command is used to enable/disable message synchronization.

Example

#Enable one-time synchronization

```
switch(config-ntp)#oncesync enable
switch(config-ntp)#
```

8.4.18 server broadcast-interval

Function

The **server broadcast-interval** command is used to configure NTP server broadcast-interval.

Format

- **server broadcast-interval { interval | default }**

Parameters

Parameters	Description	Value
interval	Specify the ntp server interval time	The value is an integer in the range from 4 to 17 (unit: s).

Default Value

The default value is 2 to 6th power seconds.

View

NTP configuration view

Usage Guidelines

Use this command to configure NTP server broadcast-interval time,

Example

Set the interval for configuring NTP server notification to 10s.

```
switch(config-ntp)#server broadcast-interval 10
switch(config-ntp)#
```

8.4.19 stratum

Function

The **stratum** command configures NTP layer-number.

Format

- **stratum { layer-number | default }**

Parameters

Parameters	Description	Value
layer-number	Set the layer number of the system clock	The value is an integer in the range from 1 to 16

Default Value

The default value is 16

View

NTP configuration view

Usage Guidelines

None

Example

#Set the stratum as 10.

```
switch(config-ntp)#stratum 10
switch(config-ntp)#
```

8.4.20 trusted-keyid {enable|disable}

Function

The trusted-keyid {enable|disable} command enables or disables MD5 **authentication key.**

Format

trusted-keyid *trusted-keyid-time* { **enable** | **disable** }

Parameters

Parameters	Description	Value
trusted-keyid-tim*e*	MD5 trusted-keyid	The value is an integer in the range from 1 to 4294967295.
enable	Enable MD5 trusted-keyid	-
disable	Disable MD5 trusted-keyid	-

Default Value

By default, MD5 **authentication key is disabled.**

View

NTP configuration view

Usage Guidelines

None

Example

Enable MD5 trusted-keyid

```
switch(config-ntp)#trusted-keyid 1 enable
switch(config-ntp)#
```

9. VXLAN Configuration Commands

9.1 Overview

This chapter introduces VXLAN configuration of the N-series switch.

9.1.1 arp broadcast-suppress {enable|disable}

Function

The **arp broadcast-suppress enable** command enables ARP broadcast suppress in a BD.
The **arp broadcast-suppress disable** command disables ARP broadcast suppress in a BD.

Format

- **arp broadcast-suppress enable**
- **arp broadcast-suppress disable**

Parameters

None

Default Value

Arp broadcast suppression is disabled in BD.

View

BD view

Usage Guidelines

If a gateway receives a large number of ARP requests within a short period and broadcasts the ARP requests in a BD, excessive ARP requests are forwarded.

Example

Enable ARP broadcast-suppression in BD 1.

```
switch(config)#bridge-domain 1
switch(config-bridge-domain-1)#arp broadcast-suppress enable
```

Disable ARP broadcast-suppression in BD 1.

```
switch(config)#bridge-domain 1
switch(config-bridge-domain-1)#arp broadcast-suppress disable
```

9.1.2 arp collect-host {enable|disable}

Function

The **arp collect-host enable** command enables BGP EVPN to collect host information by BD.
The **arp collect-host disable** command disables BGP EVPN from collect host information by BD.

Format

- **arp collect-host enable**
- **arp collect-host disable**

Parameters

None

Default Value

BGP EVPN is disabled from collecting host information by BD.

View

BD view

Usage Guidelines

Layer 2 proxy ARP is a method that helps release the pressure on processing ARP packets.

Example

Enable BGP EVPN to collect host information by BD

```
switch(config)#bridge-domain 1
switch(config-bridge-domain-1)#arp collect-host enable
```

Disable BGP EVPN to collect host information by BD

```
switch(config)#bridge-domain 1
switch(config-bridge-domain-1)#arp collect-host disable
```

9.1.3 arp l2-proxy {enable|disable}

Function

The **arp l2-proxy enable** command enables the gateway proxy function for an Address Resolution Protocol proxy.
The **arp l2-proxy disable** command disables the gateway proxy function for an ARP proxy.

Format

- **arp l2-proxy enable**
- **arp l2-proxy disable**

Parameters

None

Default Value

The gateway proxy function is disabled from an ARP proxy.

View

BD view

Usage Guidelines

To improve network security and avoid Layer 2 users in a BD domain from direct communication with each other, run the arp l2-proxy gateway-mac command to enable the gateway proxy function so that traffic can be diverted to the desired gateway.

Prerequistes

ARP broadcast suppression has been enabled using the arp broadcast-suppress enable command.

Example

Enable the gateway proxy function on an ARP proxy.

```
switch(config)#bridge-domain 1
switch(config-bridge-domain-1)#arp l2-proxy gateway-mac enable
```

Enable the gateway proxy function on an ARP proxy.

```
switch(config)#bridge-domain 1
switch(config-bridge-domain-1)#arp l2-proxy gateway-mac disable
```

9.1.4 bridge-domain (global configuration view)

Function

The **bridge-domain** command creates a bridge domain (BD) and displays its configuration view.
The **no bridge-domain** command deletes a BD.

Format

- **bridge-domain** *bd-id*
- **no bridge-domain**

Parameters

Parameter	Description	Value
bd-id	Specifies a BD ID.	The value is an integer ranging from 1 to 1000.

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Create BD 1 and enter its view.

```
switch(config)#bridge-domain 1
switch(config-bridge-domain-1)#
```

Related Commands

None

9.1.5 vxlan vni

Function

The **vxlan vni** command configures the VIN bound to BD.
The **no vxlan vni** command deletes the VIN bound to BD.

Format

- **vxlan vni** *vni-id*
- **no vxlan vni** *vni-id*

Parameters

Parameter	Description	Value
vni-id	Specifies a VNI.	The value is an integer ranging from 1 to 16777215.

Default Value

By default, no VNI is bound to BD.

View

BD configuration view

Usage Guidelines

None

Example

Configure VNI 1 bound to BD.

```
switch(config)#bridge-domain 1
switch(config-bridge-domain-1)#vxlan vni 1 switch(config)#bridge-domain 1
switch(config-bridge-domain-1)#vxlan vni 1
```

Related Commands

None

9.1.6 interface nve

Function

The **interface nve** command creates a network virtualization edge (NVE) interface and displays its configuration view.
The **no interface nve** command deletes an NVE interface.

Format

- **interface nve** *nve-id*
- **no interface nve** *nve-id*

Parameters

Parameter	Description	Value
nve-id	Specifies an NVE ID.	The value is an integer ranging from 1 to 2.

Default Value

None

View

Global configuration view

Usage Guidelines

None

Example

Create an NVE interface and display its configuration view.

```
switch(config)#interface nve 1
switch(config-nve-1)#
```

Related Commands

None

9.1.7 vni ucast-peer

Function

The **vni ucast-peer** command configures the VXLAN network identifier (VNI) and the peer IP address for a tunnel.
The **no vni peer** command deletes all tunnels with the specified VNI.
The **no vni ucast-peer** command deletes the tunnel with the specified VNI and peer IP address.
The **no vni all-peer** command deletes all the peers of an NVE interface (with different VNIs).

Format

- **vni** *vni-id* **ucast-peer** *peer-ip-address*
- **no vni** *vni-id* **peer**
- **no vni** *vni-id* **ucast-peer** *peer-ip-address*
- **no vni all-peer**

Parameters

Parameter	Description	Value
vni-id	Specifies a VNI value.	The value is an integer ranging from 1 to 16777215.
peer-ip-address	Specifies a peer IP address.	The value is in dotted decimal notation.

Default Value

None

View

NVE configuration view

Usage Guidelines

None

Example

Delete the tunnel with VNI 1 and peer address 2.2.2.2.

```
switch(config)#interface nve 1
switch(config-nve-1)#vni 1 ucast-peer 2.2.2.2
switch(config-nve-1)#no vni 1 peer
switch(config-nve-1)#no vni 1 ucast-peer 2.2.2.2
```

Related Commands

None

Warning:Supports one source VTEP, one remote VTEP hosted in multiple VNIs; Supports one source VTEP, different remote VTEPs hosted in multiple VNIs.

9.1.8 tunnel source

Function

The **tunnel source** command configures the source IP address of a tunnel.
The **no tunnel source** command deletes the source IP address of a tunnel.

Format

- **tunnel source** *ip-address*
- **no tunnel source**

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address.	The value is in dotted decimal notation.
vlanid	VLAN ID	The value is an integer ranging from 1 to 4094.

Default Value

None

View

NVE configuration view

Usage Guidelines

None

Example

Set the source IP address of a tunnel to 1.1.1.1.

```
switch(config)#interface nve 1
switch(config-nve-1)#tunnel source 1.1.1.1.
```

Related Commands

None

9.1.9 encapsulation {dot1q|untag|qinq|default}

Function

encapsulation { **dot1q|untag|qinq|default** } command is used to configurate a layer 2 sub-interface type.

Format

- **encapsulation {dot1q|untag|qinq|default}**

Parameters

Parameter	Description	Value
Dot1q	Configurates a layer 2 sub-interface type as dot1q encapsulation.	-
Untag	Configurates a layer 2 sub-interface type as untag encapsulation.	-
Qinq	Configurates a layer 2 sub-interface type as qinq encapsulation.	-
Default	Configurates a layer 2 sub-interface type as default encapsulation.	-

Default Value

By default, the sub-interface is indicated as an encapsulation type of dot1q.

View

Layer 2 sub-interface view.

Usage Guidelines

Each Layer 2 sub-interface can have only one encapsulation type configurated.

Example

Configurate dot1q encapsulation type on a sub-interface.

```
switch(config)# interface 100gigaethernet 1/0/1.1
switch(config-100ge1/0/1.1)#encapsulation dot1q
```

Related Commands

None

Warning: On the same sub-interface, untag encapsulation type can not be mixed with default,dot1q and qinq; default encapsulation type cannot be mixed with untag, qinq and dot1q.

9.1.10 bridge-domain bind (layer 2 sub-interface view)

Function

bridge-domain bind command is used to configurate a sub-interface bound to a bridge-domain(BD).
no bridge-domain bind command is used to remove a layer 2 sub-interface from a BD.

Format

- **bridge-domain bind** *bd-id*
- **no bridge-domain bind**

Parameters

Parameter	Description	Value
bd-id	Specifies a BD ID.	The value is an integer ranging from1 to 1000.

Default Value

By default, no layer 2 sub-interface is added to any BD

View

Layer 2 sub-interface view

Usage Guidelines

After a BD has been created, run bridge-domain bind command to add a layer 2 sub-interface to the BD in order to ensure the forwarding of service packets within the BD.

Example

Configurate a layer 2 sub-inteface add a BD.

```
switch(config)#interface 100gigaethernet 1/0/1.1
switch(config-100ge1/0/1.1)#bridge-domain bind 1
switch(config-100ge1/0/1.1)#no bridge-domain bind
```

Related Commands

None

9.1.11 encapsulation dot1q

Function

encapsulation dot1q command is used to configurate a layer 2 sub-interface encapsulated dot1q type to access packets with a specificed vlan tag.

Format

- **encapsulation dot1q** vlan-id

Parameters

Parameter	Description	Value
vlan-id	Specifies a Vlan ID	The value is an integer ranging from1 to 4094.

Default Value

By default, no specified vlan is configurated on the dot1q encapsulation type.

View

Layer 2 sub-interface view

Usage Guidelines

None

Example

Configurate a specificed vlan for dot1q encapsulation type on a layer 2 sub-interface.

```
switch(config)# interface 100gigaethernet 1/0/1.1
switch(config-100ge1/0/1.1)#encapsulation dot1q
switch(config-100ge1/0/1.1)#encapsulation dot1q 10
```

Related Commands

None

9.1.12 encapsulation qinq vid ce-vid

Function

encapsulation qinq vid ce-vid command is used to configurate a layer 2 sub-interface encapsulated qinq type to access packets with a specificed vlan tag.

Format

- **encapsulation qinq** vlan-id1 **ce-vid** vlan-id2

Parameters

Parameter	Description	Value
vlan-id1	Specifies a Vlan ID	The value is an integer ranging from1 to 4094.
vlan-id2	Specifies a Vlan ID	The value is an integer ranging from1 to 4094.

Default Value

By default, no specified vlan is configurated on the qinq encapsulation type.

View

Layer 2 sub-interface view

Usage Guidelines

None

Example

Configurate a specificed vlan for qinq encapsulation type on a layer 2 sub-interface.

```
switch(config)# interface 100gigaethernet 1/0/1.1
switch(config-100ge1/0/1.1)#encapsulation qinq
switch(config-100ge1/0/1.1)#encapsulation qinq 10 ce-vid 100
```

Related Commands

None

9.1.13 debug vxlan

Function

The **debug vxlan** command enables or disables VXLAN debugging.

Format

- **debug vxlan** { **event** | **detect** | **off** | **all** }

Parameters

Parameter	Description	Value
event	Enables debugging of VXLAN events.	-
detect	Enables debugging of VXLAN detection.	-
off	Disables VXLAN debugging.	-
all	Displays all VXLAN debugging information.	-

Default Value

None

View

Privileged user view

Usage Guidelines

None

Example

Enable debugging of VXLAN events.

```
switch#debug vxlan event
switch#
```

Related Commands

None

9.1.14show bridge-domain

Function

The **show bridge-domain** command displays information about all the configured L2 BD interfaces, including the BD interface numbers, bound VNIs, action for unknown unicast packets, whether statistics collection is enabled.
The **show bridge-domain** *domain-id* command displays the configuration of a specified L2 BD interface.

Format

- **show bridge-domain**
- **show bridge-domain** *domain-id*

Parameters

Parameter	Description	Value
domain-id	Specifies a BD ID.	The value is an integer ranging from 1 to 1000.

Default Value

None

View

Common user view, privileged user view, global configuration view

Usage Guidelines

None

Example

Display BD information.

```
switch(config)#show bridge-domain
  Interface          Vni          VAP Ports
  bd-1                 1           100ge-1/0/1.1
```

Related Commands

None

9.1.15 show vxlan vni

Function

The **show vxlan vni** command displays VNI information.

Format

- **show vxlan vni**
- **show vxlan vni** *vni-id*

Parameters

Parameter	Description	Value
vni-id	Specifies a VNI value.	The value is an integer ranging from 1 to 16777215.

Default Value

None

View

Privileged user view, global configuration view

Usage Guidelines

None

Example

Display VNI information.

```
switch(config)#show vxlan vni
  Vni        BD                    NVE                   proto
1          N/A                   N/A                   bgp
```

Related Commands

None

9.1.16show vxlan resource

Function

The **show vxlan resource** command displays information about VXLAN resources.

Format

show vxlan resource

Parameters

None

Default Value

None

View

Privileged user view, global configuration view

Usage Guidelines

None

Example

Display information about VXLAN resources.

```
switch#show vxlan resource
 UDP port                    :4789
 Peer detect interval    :5s
 Max vni number              :4094
 Used vni number             :0
 Max peer number              :4094
 Used peer number             :0
```

```
switch#
```

Related Commands

None

9.1.17 show nve peer

Function

The **show nve peer** command displays information about all NVE peers or filtered information.

Format

- **show nve peer**
- **show nve peer verbose**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view

Usage Guidelines

None

Example

Display NVE peer information.

```
switch(config-nve-1)#show nve peer
  Interface          Vni        Peer                          State
  nve-1               100        2.2.2.2                       down
```

Related Commands

None

9.1.18 show interface nve

Function

The **show interface nve** command displays NVE information on interfaces.

Format

- **show interface nve**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view

Usage Guidelines

None

Example

Display NVE information on interfaces.

```
switch(config)#show interface nve
  Interface            SrcIP          VAP Ports
  nve-1                  1.1.1.1
```

Related Commands

None

9.1.19show ip arp vxlan

Function

The **show ip arp vxlan** command displays VXLAN ARP information.

Format

show ip arp vxlan

Parameters

None

Default Value

None

View

Common user view

Usage Guidelines

None

Example

Display VXLAN ARP information on the switch.

```
switch#show ip arp vxlan
  ------------------------------------------------------------------------------------
  Total: 0          Dynamic: 0          Static: 0          Other: 0
switch#
```

9.1.20 show ip bgp evpn route

Function

The **show ip bgp evpn route** command displays BGP EVPN route information.

Format

- **show ip bgp evpn route**
- **show ip bgp evpn route { mac-ip| prefix | tunnel }**
- **show ip bgp evpn route arp ip-address**
- **show ip bgp evpn route count**
- **show ip bgp evpn route mac mac-address**
- **show ip bgp evpn route nd ipv6-address**
- **show ip bgp evpn route prefix ip-address**
- **show ip bgp evpn route tunnel tunnel-source-ip-address tunnel-vni**

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address.	The value is in dotted decimal notation.
mac-address	Specifies the destination MAC address.	for example, AA:BB:CC:DD:EE:FF
ipv6-address	Specifies the IPv6 address of a neighbor.	-
tunnel-source-ip-address	Specifies the tunnel-source-ip-address	The value is in dotted decimal notation.
tunnel-vni	Specifies the tunnel-vni	The value is an integer ranging from 1 to 1000000

Default Value

None

View

Common user view

Usage Guidelines

None

Example

displays BGP EVPN route information.

```
switch#show ip bgp evpn route
switch#
```

9.1.21show ipv6 nd l2-proxy

Function

The **show ipv6 nd l2-proxy** command shows dynamic proxy ND entries in a specified BD.

Format

- **show ipv6 nd l2-proxy**
- **show ipv6 nd l2-proxy interface config**

Parameters

None

Default Value

None

View

Common user view

Usage Guidelines

None

Example

shows dynamic proxy ND entries in a specified BD.

```
switch#show ipv6 nd l2-proxy
switch#
```

9.1.22 unknown-ucast {forward|drop}

Function

The **unknown-ucast {forward|drop}** command configures the processing of unknown ucast packets during the BD packet forwarding.

Format

- **unknown-ucast { forward | drop }**

Parameters

Parameters	Description	Value
forward	Forwards unknown multicast packets.	-
drop	Drops unknown multicast packets.	-

Default Value

None

View

BD configuration view

Usage Guidelines

None

Example

Configure BD node to directly discard unknown multicast packets.

```
switch(config-bridge-domain-1)#unknown-ucast forward
switch(config-bridge-domain-1)#
```

9.1.23 vxlan anycast-gateway {enable|disable}

Function

The **vxlan anycast-gateway {enable|disable}** command enables or disable the distributed gateway function.

Format

- **vxlan anycast-gateway { enable | disable }**

Parameters

Parameters	Description	Value
enable	Enable the distributed gateway function.	-
disable	Disable the distributed gateway function.	-

Default Value

By default, the distributed gateway function is disabled.

View

BD configuration view

Usage Guidelines

None

Example

Enable the distributed gateway function.

```
switch(config)#bridge-domain 1
switch(config-bridge-domain-1)#quit
switch(config)#interface bridge-domain 1
switch(config-bridge-domain1)#vxlan anycast-gateway enable
switch(config-bridge-domain1)#
```

9.1.24 debug ipv6 nd l2-proxy

Function

The **debug ipv6 nd l2-proxy** command enables information debugging about the proxy ND table in a specified BD.
The **debug ipv6 nd l2-proxy** command disables information debugging about the proxy ND table in a specified BD.

Format

- **debug ipv6 nd l2-proxy**
- **no debug ipv6 nd l2-proxy**

Parameters

None

Default Value

Disable

View

privileged user view

Usage Guidelines

None

Example

enables information debugging about the proxy ND table in a specified BD.

```
switch#debug ipv6 nd l2-proxy
switch#
```

9.1.25 reset vxlan statistics peer-ip

Function

The **reset vxlan statistics peer-ip** command clears VXLAN tunnel packet statistics.

Format

- **reset vxlan statistics peer-ip ip-address**
- **reset vxlan statistics peer-ip ip-address vpn-instance name**

Parameters

Parameters	Description	Value
ip-address	Specifies the IP address of the remote VTEP.	The value is in dotted decimal notation.
name	Specifies the VPN instance	The value is a character string.

Default Value

None

View

global configuration view

Usage Guidelines

None

Example

Cleared VXLAN packet statistics

```
switch(config)#reset vxlan statistics peer-ip 10.1.1.1
switch(config)#
```

9.1.26 debug trace vxlan

Function

The **debug trace vxlan** command enables VXLAN tunnel debugging .
The **no debug trace vxlan** command disables VXLAN tunnel debugging .

Format

- **debug trace vxlan**
- **no debug trace vxlan**

Parameters

None

Default Value

Disable

View

privileged user view

Usage Guidelines

None

Example

enables VXLAN tunnel debugging .

```
switch#debug trace vxlan
switch#
```

9.1.27 ping vxlan vni source peer

Function

ping vxlan vni source peer command detects the connectivity of the VXLAN tunnel and specifies the source IP address and peer ip address of the VXLAN.

Format

- **ping vxlan vni vni-id source ip-address peer peer-ip-address [string]**

Parameters

Parameters	Description	Value
vni-id	vni id	The value is an integer ranging from 1 to 16777215.
ip-address	Specifies the source IP address	The value is in dotted decimal notation.
peer-ip-address	Specifies the peer IP address	The value is in dotted decimal notation.
string	Specifies the string	-t|-n|<1-4294967295>|-m|<1-10000>|-w|<0-65535>|-tos|<0-255>|-a|A.B.C.D|udp-port|<1-65535>|-vpn-instance|VPNNAME|NAMECR

Default Value

None

View

privileged user view

Usage Guidelines

None

Example

Detect the connectivity of the VXLAN tunnel and specify the source IP address and peer ip address of the VXLAN.

```
switch#ping vxlan vni 1 source 1.1.1.1 peer 3.3.3.3
switch#
```

9.1.28 trace vxlan vni source peer

Function

trace vxlan vni source peer command traces the connectivity of the VXLAN tunnel and specifies the source IP address and peer ip address of the VXLAN.

Format

- **trace vxlan vni** *vni-id* **source** *ip-address* **peer** *ip-address* { **-w** *wati-value* | **-h** *max-ttl* | **-a** *echo-ip-address* | **udp-port** *udp-port-number*}

Parameters

Parameters	Description	Value
vni-id	vni id	The value is an integer ranging from 1 to 16777215
ip-address	Specifies the source IP address	The value is in dotted decimal notation.
-w	Specifies the timeout period to wait for an ICMP Echo Reply message after an ICMP Echo Request message is sent.	The value is an integer ranging from 0 to 65535 (unit: ms).The default value is 2000 ms
-h	Specifies the max value of TTL	The value is an integer ranging from 1 to 255
-a	Specifies the source ip address of ICMP echo request as the default outbound interface IP address.	The value is in dotted decimal notation.
udp-port-number	Specifies udp-port-number	The value is an integer ranging from 1 to 65535

Default Value

None

View

privileged user view

Usage Guidelines

None

Example

Traces the connectivity of the VXLAN tunnel and specifies the source IP address and peer ip address of the VXLAN.

```
switch#trace vxlan vni 1 source 1.1.1.1 peer 1.1.1.10 –h 125
switch#
```

9.1.29 rewrite egress vid

Function

The **rewrite egress vid** command changes the VLAN tag that a Layer 2 sub-interface using Dot1q encapsulation adds to packets when decapsulating the packets.
The **no rewrite egress vid** command restores the VLAN tag that a Layer 2 sub-interface using Dot1q encapsulation adds to packets when decapsulating the packets.

Format

- **rewrite egress vid vlan-id**
- **no rewrite egress vid**

Parameters

Parameters	Description	Value
vlan-id	Specifies the VLAN tag that a Layer 2 sub-interface using Dot1q encapsulation adds to packets when decapsulating the packets.	It is an integer ranging from 1 to 4094.

Default Value

None

View

Ethernet sub-interface view、Trunk sub-interface view

Usage Guidelines

No

Example

Change the VLAN tag to be added to packets when the packets are decapsulated to 20 on the Layer 2 sub-interface 10GE1/0/1.1.

```
switch(config-10ge1/0/1.1)#rewrite egress vid 20
switch(config-10ge1/0/1.1)#
```

9.1.30 rewrite no-action

Function

The **rewrite no-action** command configures a dot1q Layer 2 sub-interface to transparently transmit received packets, instead of removing VLAN tags from the packets.
The **no rewrite no-action** command restores the default configuration.

Format

- **rewrite no-action**
- **no rewrite no-action**

Parameters

None

Default Value

None

View

Enterprise sub-interface configuration view、Trunk2 sub-interface configuration view

Usage Guidelines

None

Example

Configure the Layer 2 sub-interface 10GE 1/0/1.1 to transparently transmit received packets.

```
switch(config-10ge1/0/1.1)#rewrite no-action
switch(config-10ge1/0/1.1)#
```

9.1.31rewrite pop double

Function

The **rewrite pop double** command enables a Layer 2 sub-interface with the encapsulation type being QinQ to remove double VLAN tags from received packets.
The **no rewrite pop double** command disables a Layer 2 sub-interface with the encapsulation type being QinQ from removing double VLAN tags from received packets.

Format

- **rewrite pop double**
- **no rewrite pop double**

Parameters

None

Default Value

None

View

Enterprise sub-interface configuration view、Trunk2 sub-interface configuration view

Usage Guidelines

None

Example

Enable 10GE 1/0/1.1 to remove double tags from received packets.

```
switch(config-10ge1/0/1.1)#rewrite pop double
switch(config-10ge1/0/1.1)#
```

9.1.32 debug evpn

Function

The **debug evpn** command enables or disables **evpn** debugging.

Format

- **debug evpn { error|nm|event|all }**

Parameters

Parameters	Description	Value
event	Enables debugging of EVPN events.	-
nm	Enable debugging of management configuration	-
error	Enables debugging of EVPN errors	-
all	Displays all EVPN debugging information.	-

Default Value

None

View

privileged user view

Usage Guidelines

None

Example

Enable the evpn function on the switch.

```
switch#debug evpn event
switch#
```

9.1.33 debug bgp

Function

The **debug bgp** command enables **bgp** debugging.
The **no debug bgp** command disables **bgp** debugging.

Format

- **debug bgp { update | rib-tree | route | event | tcp | packet | all | orf | graceful-restart | socket }**
- **no debug bgp { update | rib-tree | route | event | tcp | packet | all | orf | graceful-restart | socket }**

Parameters

Parameter	Description	Value
update	Enable debugging of updating information.	-
rib-tree	Enable debugging of rib tables.	-
route	Enable debugging of route information.	-
event	Enable debugging of event information.	-
tcp	Enable debugging of TCP information.	-
packet	Enable debugging of packet information.	-
all	Indicates all of the preceding debug information.	-
orf	Enable debugging of orf information.	-
graceful-restart	Enable debugging of graceful-restart information.	-
socket	Enable debugging of socket information.	-

Default Value

None

View

privileged user view

Usage Guidelines

None

Example

Enable debugging of BGP orf information.

```
switch#debug bpg orf
switch#
```

9.1.34 evpn

Function

The **evpn** command is used to create an EVPN instance in VXLAN mode.
The **no evpn** command is used to delete an EVPN instance in VXLAN mode.

Format

- **evpn**
- **no evpn**

Default Value

None

View

BD configuration view

Usage Guidelines

None

Example

create an EVPN instance in VXLAN mode.

```
switch(config)#bridge-domain 2
switch(config-bridge-domain-2)#evpn
switch(config-bridge-domain-2)#
```

9.1.35 evpn-family

Function

The **evpn-family** command enters address family views of BGP-EVPN.

Format

- **evpn-family**

Default Value

None

View

BD configuration view

Usage Guidelines

None

Example

Enter the address family views of BGP-EVPN.

```
switch(config-bgp)#evpn-family
switch(config-bgp-af-evpn)#
```

9.1.36 evpn route-distinguisher

Function

The **evpn route-distinguisher** command configures a route distinguisher (RD) for a BD EVPN instance.

Format

- **evpn route-distinguisher RDSTRING**

Parameters

Parameter	Description	Value
RDSTRING	Specifies an RD to be configured for a BD EVPN instance.	The format of an RD can be as follows: 2-byte AS number:4-byte user-defined number, for example, 1:3. An AS number is an integer ranging from 0 to 65535, and a user-defined number is an integer ranging from 0 to 4294967295. The AS and user-defined numbers cannot be both 0s. This means that an RD cannot be 0:0. Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number is an integer ranging from 65536 to 4294967295, and a user-defined number is an integer ranging from 0 to 65535. 4 -byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of x.y, where x and y are integers ranging from 0 to 65535. A user-defined number is an integer ranging from 0 to 65535. The AS and user-defined numbers cannot be both 0s. This means that an RD cannot be 0.0:0. 32-bit IP address:2-byte user-defined number. For example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255, and a user-defined number is an integer ranging from 0 to 65535.

Default Value

By default, no RD is configured for BD EVPN instances.

View

BD configuration view

Usage Guidelines

None

Example

#configures a route distinguisher (RD) for a BD EVPN instance.

```
switch(config)#bridge-domain 2
switch(config-bridge-domain-2)#evpn route-distinguisher 1:1
switch(config-bridge-domain-2)#
```

9.1.37 evpn vpn-target

Function

The **evpn vpn-target** command configures VPN targets for a BD EVPN instance.
The **no evpn vpn-target** command deletes the VPN targets of a BD EVPN instance.

Format

- **evpn vpn-target TARGET {both|export-extcommunity|import-extcommunity}**
- **no evpn vpn-target TARGET { both|export-extcommunity|import-extcommunity}**
- **no evpn vpn-target**

Parameters

Parameter	Description	Value
TARGET	Specifies a VPN target to be configured for a BD EVPN instance.	The format of a VPN target can be as follows: 2-byte AS number:4-byte user-defined number, for example, 1:3. An AS number is an integer ranging from 0 to 65535, and a user-defined number is an integer ranging from 0 to 4294967295. The AS and user-defined numbers cannot be both 0s. This means that a VPN target cannot be 0:0. Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number is an integer ranging from 65536 to 4294967295, and a user-defined number is an integer ranging from 0 to 65535. 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of x.y, where x and y are integers ranging from 0 to 65535. A

Parameter	Description	Value
		user-defined number is an integer ranging from 0 to 65535. The AS and user-defined numbers cannot be both 0s. This means that a VPN target cannot be 0.0:0. 32-bit IP address:2-byte user-defined number. For example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255, and a user-defined number is an integer ranging from 0 to 65535.
both	Adds a VPN target to both the import and export VPN target lists of a BD EVPN instance.	-
export-extcommunity	Adds a VPN target to the export VPN target list of a BD EVPN instance.	-
import-extcommunity	Adds a VPN target to the import VPN target list of a BD EVPN instance.	-

Default Value

None

View

BD configuration view

Usage Guidelines

None

Example

configures VPN targets for a BD EVPN instance.

```
switch(config)#bridge-domain 2
switch(config-bridge-domain-2)#evpn vpn-target 1:1 import-extcommunity
switch(config-bridge-domain-2)#
```

9.1.38 neighbor enable

Function

The **neighbor enable** command enables the neighbor checking of EVPN address family.

Format

- **neighbor ipv4 address enable**

Parameters

Parameter	Description	Value
ipv4 address	Specifies the IPv4 address of BGP neighbor.	The value is in dotted decimal notation.

Default Value

By default, EVPN is disabled.

View

BGP-EVPN address family configuration view

Usage Guidelines

None

Example

enables the neighbor checking of EVPN address family

```
switch (config-bgp-af-evpn)#neighbor 2.2.2.2 enable
switch (config-bgp-af-evpn)#
```

9.1.39 vni replication-protocol

Function

The **vni replication-protocol** command configures an ingress replication list that contains the IP addresses of those remote VTEPs for a VXLAN network identifier (VNI).

Format

- **vni vni-id replication {bgp}**

Parameters

Parameter	Description	Value
vni-id	Specifies a VNI ID number.	The value is an integer ranging from 1 to 16777215.
bgp	Specifies BGP to create a vxlan tunnel.	-

Default Value

None

View

NVE configuration view

Usage Guidelines

None

Example

#Specify the VNI to create a vxlan tunnel through BGP on the nve interface.

```
switch(config-nve-1)#vni 10 replication-protocol bgp
switch(config-nve-1)#
```

9.1.40 vxlan vni

Function

The **vxlan vni** command configures the VNI bound to VPN instance.

Format

- **vxlan vni vni-id**

Parameters

Parameter	Description	Value
vni-id	Specifies a VNI ID number.	The value is an integer ranging from 1 to 16777215.

Default Value

None

View

VPN configuration view

Usage Guidelines

None

Example

configures the VNI bound to VPN instance.

```
switch(config)#ip vpn-instance 111
switch(config-vpn-instance-111)#vxlan vni 1
```

9.1.41show evpn

Function

The **show evpn** command displays EVPN information.

Format

- **show evpn**
- **show evpn bridge-domain evpn**

Parameters

Parameter	Description	Value
evpn	Specifies a Bridge-domain ID	The value is an integer ranging from 1 to 16777215.

Default Value

None

View

common user view

Usage Guidelines

None

Example

Display EVPN information.

```
switch(config)# show evpn
EVPN    RD
1       1:1
2       2:2
```

9.1.42 show evpn vpn-target

Function

The **show evpn vpn-target** command displays EVPNvpn-target information.

Format

- **show evpn vpn-target**

Parameters

None

Default Value

None

View

common user view

Usage Guidelines

None

Example

Display EVPN vpn-target information.

```
switch(config)# show evpn vpn-target
EVPN    VPN-TARGET    Type
1           1:1                import-extcommunity
1           1:1                export-extcommunity
```

10. VPN Commands

10.1 Overview

This chapter introduces the operation and maintenance configuration commands of the N-series switch.

10.2 L3VPN Configuration Commands

10.2.1debug l3vpn

Function

The **debug l3vpn** command enables L3VPN debugging.
The **no debug l3vpn** command disables L3VPN debugging.

Format

- **debug l3vpn { io | event | error | nm | all }**
- **no debug l3vpn { io | event | error | nm | all }**

Parameters

None

Default Value

By default, L3VPN debugging is disabled.

View

privileged user view

Usage Guidelines

Use this command enable and maintain L3VPN debugging.

Example

enables L3VPN debugging.

```
switch#debug l3vpn all
switch#
```

10.2.2 description

Function

The **description** command specifies the description of the current VPN instance.
The **no description** command deletes the description of the current VPN instance.

Format

- **description description-information**
- **no description**

Parameters

Parameters	Description	Value
description-information	Specifies the description of a VPN instance.	The value is a string of 1 to 30 case-sensitive characters

Default Value

By default, no description is specified for a VPN instance.

View

IP-VPN configuration view

Usage Guidelines

If you run the description command several times, the latest configuration overrides the previous configurations.

Example

Specify the description of a VPN instance named vpn1.

```
switch(config-vpn-instance-111)#description fhn
switch(config-vpn-instance-111)#
```

10.2.3 ip binding vpn-instance

Function

The **ip binding vpn-instance** command associates an interface on a VLAN with a VPN instance.
The no ip binding vpn-instance command disables the association an interface on a VLAN with a VPN instance.

Format

- **ip binding vpn-instance vpn-instance-name**
- **no ip binding vpn-instance vpn-instance-name**

Parameters

Parameters	Description	Value
vpn-instance-name	Specifies the name of the VPN instance	The value is a string of 1 to 31 case-sensitive characters

Default Value

By default, an interface is a VLAN interface and is not associated with any VPN instance.

View

VLANIF configuration view, Loopback interface configuration view, Tunnel interface configuration view, bd interface configuration view、enterprise interface configuration view、grp route interface configuration view

Usage Guidelines

None

Example

After a VPN instance is created, you need to associate the VLANIF2 interface connecting to the VPN with the VPN instance.

```
switch(config-vlanif-2)#ip binding vpn-instance 111
switch(config-vlan-2)#
```

10.2.4 ipv4-family|ipv6-family

Function

The **ipv4-family|ipv6-family** command enables the IPv4 or IPv6 address family for a VPN instance and displays the VPN instance IPv4 or IPv6 address family view.
The **no ipv4-family|ipv6-family** command disables the IPv4 or IPv6 address family for a VPN instance.

Format

- **ipv4-family**
- **ipv6-family**
- **no ipv4-family**
- **no ipv6-family**

Parameters

None

Default Value

None

View

VPN configuration view

Usage Guidelines

None

Example

displays the VPN instance IPv4 or IPv6 address family view.

```
switch(config-vpn-instance-111)#ipv4-family
switch(config-vpn-instance-111-af-ipv4)#
```

10.2.5 vpn-target

Function

The **vpn-target** command configures VPN target extended community attribute for the VPN instance address family.
The **no vpn-target** command deletes the setting.

Format

- **vpn-target target { both | export-extcommunity | import-extcommunity }**
- **no vpn-target**
- **no vpn-target target { both | export-extcommunity | import-extcommunity }**

Parameters

Parameters	Description	Value
target	Specifies the VPN target extended community attribute to be added to the VPN target extended community list of the VPN instance address family.	16-byte AS number: 32-byte user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0s. That is, the VPN target cannot be 0:0. IPv4-address: 16-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. 32-byte AS number in dotted notation:16-byte user-defined number, for example, 100:5:1. A 32-byte AS number in dotted notation is in the format of x.y, where x and y are integers that range from 0 to 65535. The user-defined number also ranges from 0 to 65535. The AS number and user-defined number cannot both be 0s. That is, the VPN target cannot be 0.0:0.
both	Adds the VPN target extended community attribute to the export and import VPN target extended community lists of the VPN instance address family.	-
export-extcommunity	Adds the VPN target extended community attribute to the export VPN target extended community lists of the VPN instance address family.	-
import-extcommunity	Adds the VPN target extended community attribute to the import VPN target extended community lists of the VPN instance address family.	-

Default Value

None

View

ip-vpn-af-ipv4 configuration view, ip-vpn-af-ipv6 configuration view

Usage Guidelines

If a VPN instance is configured on a PE, the vpn-target command must be used to configure a VPN target for the address family of the VPN instance.

Example

configure a VPN target for the the L2VPN instance named VPN1 .

```
switch(config-vpn-instance-111)#ipv4-family
switch(config-vpn-instance-111-af-ipv4)#vpn-target 1:100 export-extcommunity
switch(config-vpn-instance-111-af-ipv4)#
```

10.2.6 route-distinguisher

Function

The **route-distinguisher** command configures a route distinguisher (RD) for a VPN instance address family.

Format

- **route-distinguisher rdstring**

Parameters

Parameters	Description	Value
rdstring	Specifies the value of an RD.Adds the VPN target extended community attribute to the export or import VPN target extended community lists of the VPN instance address family.	16-byte AS number: 32-byte user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0s. That is, the VPN target cannot be 0:0. IPv4-address: 16-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. 32-byte AS number in dotted notation:16-byte user-defined number, for example, 100:5:1. A 32-byte AS number in dotted notation is in the format of x.y, where x and y are integers that range from 0 to 65535. The user-defined number also ranges from 0 to 65535. The AS number and user-defined number cannot both be 0s. That is, the VPN target cannot be 0.0:0.

Default Value

None

View

ip-vpn-af-ipv4 configuration view, ip-vpn-af-ipv6configuration view

Usage Guidelines

After an RD is deleted, all configurations in the VPN instance IPv4 address family or the IPv6 address family of the corresponding VPN instance will be deleted.

Example

Configure an RD for the VPN instance named 100:4.

```
switch(config-vpn-instance-111)#ipv4-family
switch(config-vpn-instance-111-af-ipv4)#route-distinguisher 100:4
switch(config-vpn-instance-111)#
```

10.2.7 show ip vpn-instance

Function

The **show ip vpn-instance** command displays configurations of VPN instances.

Format

- **show ip vpn-instance**

Parameters

None

Default Value

None

View

Common user view

Usage Guidelines

Parameters	Description	Value
VPN-Instance Name	Specifies the name of a VPN instance.	-
RD	Specifies the threshold for the number of routes.	-
Creation Time	Creation Time for VPN instance.	-

Example

show VPN instance details.

```
switch#show ip vpn-instance
 Total VPN-Instances configured : 2
 VPN-Instance Name                RD                        Creation Time
 1                                                          2019-02-09 13:44:01
 2                                                          2019-02-09 14:17:48
switch#
```

10.2.8 show ip vpn-instance verbose

Function

The **show ip vpn-instance verbose** command is used to show detail VPN instance.

Format

- **show ip vpn-instance verbose**
- **show ip vpn-instance name verbose**

Parameters

Parameters	Description	Value
name	Specifies the name of a VPN instance.	The value is a string of 1 to 31

Default Value

None

View

Common user view

Usage Guidelines

The description of show detail VPN instance is as follows:

Parameters	Description
VPN-Instance Name	Display the name of a VPN instance and VPN ID
Creation Time	Time created by VPN instance
Route Distinguisher	Route Distinguisher（RD）
description	Specifies the information of a VPN instance.
Apply Label Per Instance	Specifies the apply Label Per Instance
VPN Target	VPN Target

Example

Display the information of a VPN instance.

```
switch#show ip vpn-instance verbose
VPN-Instance Name and ID: 1, 1
   Creation Time: 2017-02-09 13:44:01
   Route Distinguisher:
   Description: --
   Apply Label Per Instance: Disable
VPN-Instance Name and ID: 2, 2
   Creation Time: 2017-02-09 14:17:48
   Route Distinguisher:
   Description: --
   Apply Label Per Instance: Enable
switch#
```

10.2.9 show ip vpn-instance config

Function

The **showip vpn-instance config** command displays the VPN instance configuration information.

Format

- **show ip vpn-instance config**

Parameters

None

Default Value

None

View

Common user view

Usage Guidelines

None

Example

displays the VPN instance configuration information.

```
switch#show ip vpn-instance config
 ip vpn-instance 1
 description testvpn1
 ip vpn-instance 2
 apply-label per-instance
```

```
switch#
```

10.2.10 show ip vpn-instance import-vt

Function

The **show ip vpn-instance import-vt** command displays all VPN instances with the specified import vpn-target attribute.

Format

- **show ip vpn-instance import-vt target**

Parameters

Parameters	Description	Value
target	Specifies the value of the import VPN-target attribute.	16-byte AS number: 32-byte user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a VPN target cannot be 0:0. IPv4-address: 32-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. 32-byte AS number in dotted notation is in the format of x.y, where x and y are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.

Default Value

None

View

Common user view

Usage Guidelines

The value of the parameter target in this command can be expressed in one of three formats:
IP<X.X.X.X>:NN<0-65535>

Display 16-byte AS number: 32-byte user-defined number, for example, 10.18.12.15:1The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535.
AS<0-65535>:NN<0-4294967295>
Display 16-byte AS number: 32-byte user-defined number, for example, 1:5. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a VPN target cannot be 0:0.
AS<0-65535>.<0-65535>:NN<0-65535>
Display32-byte AS number :16-byte user-defined number in dotted notation is in the format of x.y,for example, 10.2:1. where x and y are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.

Example

displays all VPN instances with the specified import vpn-target attribute.

```
switch#show ip vpn-instance import-vt 100:1
The vpn-instances are :
  VPN-Instance Name and ID : vpn1, 1
  VPN-Instance Name and ID : vpn2, 2
  VPN-Instance Name and ID : vpn28, 3
```

10.2.11 route-distinguisher

Function

The **route-distinguisher** command configures a route distinguisher (RD) for a VPN instance address family.
The **no route-distinguisher** command deletes the RD configuration in a specified VPN instance address family.

Format

- **route-distinguisher RDSTRING**
- **no route-distinguisher**

Parameters

Parameters	Description	Value
RDSTRING	Specifies the value of an RD.	The forms of RD are as follows: 2-byte AS number: 4-byte user-defined number, for example, 1:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot be 0s at the same time. That is, an RD cannot be 0:0. Integral 4-byte AS number: 2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0.

Default Value

By default, no RD is configured for the VPN instance address family.

View

VPN instance IPv4 address family view, VPN instance IPv6 address family view

Usage Guidelines

None

Example

configure an RD for the VPN instance address family.

```
switch(config-vpn-instance)#ipv4-family
switch(config-vpn-instance-af-ipv4)#route-distinguisher 22:1
switch(config-vpn-instance-af-ipv4)#
```

11. Operation and Maintenance Commands

11.1 Overview

This chapter introduces the operation and maintenance configuration commands of the N-series switch.

11.2 RMON Configuration Commands

11.2.1 rmon alarm

Function

The **rmon alarm** configures RMON alarm entries.
The **no rmon alarm** deletes RMON alarm entries.

Format

- **rmon alarm** *alarm-id object-id query-interval* { **absolute** | **delta** } *rising-threshold rising-event falling-threshold falling-event* [*owner*]
- **no rmon alarm** *alarm-id*

Parameters

Parameters	Description	Value
alarm-id	Specifies the ID of an RMON alarm entry.	The value is an integer in the range from 1 to 65535.
object-id	Specifies an alarm object ID (only a variable that can be resolved to an integer in ASN.1 can be used as an alarm object ID).	The value is a character string in the dotted node OID format, such as 1.3.6.1.2.1.2.2.1.8.2.
query-interval	Specifies the interval for alarm query.	The value is an integer in the range from 2 to 2000000 (unit: s).
{ absolute | delta }	Indicates an absolute value or a relative value (increment).	-
rising-threshold	Indicates the rising threshold.	The value is an integer in the range from 0 to 4294967295.
rising-event	Indicates the rising event entry number.	The value is an integer in the range from 0 to 65535.
falling-threshold	Indicates the falling threshold.	The value is an integer in the range from 0 to 4294967295.
falling-event	Indicates the falling event entry number.	The value is an integer in the range from 0 to 65535.
[owner]	Defines an RMON alarm user (optional).	The value is a string of 0 to 127 characters.

Default Value

None

View

Global configuration view

Usage Guidelines

When adding an alarm table entry using this command, configure the source object ID, query interval, alarm sample type, alarm generation type, and the corresponding time. In this way, the system can determine whether to record an alarm event in a log or send a trap message to the NMS in case of alarm events.
The sample types can be obtained in the following methods: Compare the relative value (current sample value minus the last sample value) with the threshold; compare the absolute value (current sample value) with the threshold. The comparison result is used to generate the rising or falling event.

Example

Configure an RMON alarm entry.

```
switch(config)#rmon alarm 1 1.3.6.1.2.1.2.2.1.8.2 2 absolute 1 1 2 1
switch(config)#
```

11.2.2 rmon event

Function

The **rmon event** command is used to configure an RMON event control entry.
The **no rmon event** command is used to delete an RMON event control entry.

Format

- **rmon event** *event-id* { **log** | **trap** | **both** } [*description*]
- **no rmon event** *event-id*

Parameters

Parameters	Description	Value
event-id	Specifies the ID of an RMON event control entry.	The value is an integer in the range from 1 to 65535.
{ log|trap|both }	Specifies the event type. log: A switch generates event logs. trap: A switch generates event alarms. both: A switch generates both event logs and alarms.	-
[description]	Specifies the event description (optional).	The value is a character string.

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to configure the event ID and event processing mode, so that a switch can handle the alarm events accordingly.

Example

Configure an RMON event control entry.

```
switch(config)#rmon event 1 both CLI
switch(config)#
```

11.2.3 show rmon alarm

Function

The **show rmon alarm** command is used to show the configuration of an RMON alarm control entry.

Format

- **show rmon alarm**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

You can use this command to view configuration information of an RMON alarm control entry, including the alarm ID, alarm query interval, rising threshold, and falling threshold.

Example

Show the configuration of an RMON alarm control entry.

```
switch#show rmon alarm
RMON Event 1 log successedarm
```

```
  RMON Alarm:1
        Interval:2
        Source OID:1.3.6.1.2.1.2.2.1.8.2
        Sample Type:absolute value
        Alarm Value:2
        Startup Alarm:risingOrFallingAlarm
        Rising Threshold:1
        Rising Event:1
        Falling Threshold:2
        Falling Event:1
        Owner:CLI
        Status:valid
switch#
```

11.2.4show rmon config

Function

The **show rmon config** command is used to show the configuration of an RMON event.

Format

- **show rmon config**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

You can use this command to show the configuration of an RMON event.

Example

Show the configuration of an RMON event.

```
switch#show rmon config
!
!Rmon configuration
 rmon event 1 log
 rmon event 2 both
```

```
switch#
```

11.2.5 show rmon event

Function

The **show rmon event** command is used to show the configuration of an RMON event control entry.

Format

- **show rmon event**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

You can use this command to show the configuration of an RMON event control entry, including the event control entry ID, description information, type, and last transmit time.

Example

Show the configuration of an RMON event control entry.

```
switch#show rmon event
  RMON Event:1
        Type:log
        Status:valid
        Lastsent time:0 days 0 hours 0 minutes 0 seconds
        Description:N/A
        Owner:N/A
  RMON Event:2
        Type:trap&log
        Status:valid
        Lastsent time:0 days 0 hours 0 minutes 0 seconds
        Description:N/A
        Owner:N/A
switch#
```

11.2.6show rmon history

Function

The **show rmon history** command shows the configuration of an RMON historical record control entry.

Format

- **show rmon history** [*history-id*]

Parameters

Parameters	Description	Value
history-id	Specifies the ID of an RMON historical record control entry.	The value is an integer in the range from 1 to 127.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

You can use this command to show the configuration of an RMON historical record control entry. If *history-id* is not included, the system shows the configuration of all historical record control entries. Otherwise, the system shows the configuration information of the historical record control entry with the specified ID.

Example

Show the configuration of an RMON historical record control entry.

```
switch#show rmon history
  'BR' means 'Buckets Requested'
  'BG' means 'Buckets Granted'
  'DS' means 'Data Source'
  'ACT' means 'Active
  'UC' means 'Undercreation'
  RMON ethernet statistics
  Index BR      BG      Interval State DS
  1       20      20      300         ACT     ifIndex.2
switch#

switch#show rmon history 1
  RMON history control:1
          History Data Source ifIndex.2
```

```
        Buckets Requested : 20
        Buckets Granted : 20
        Interval : 300
        Owner : cli
        Status : valid
switch#
```

11.2.7 show rmon history statistics

Function

The **show rmon history statistics** command is used to show statistics on RMON historical record control entries.

Format

- **show rmon history statistics**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

You can use this command to show statistics on RMON historical record control entries.

Example

Show statistics on RMON historical record control entries.

```
switch#show rmon history statistics
  RMON History statistics:1/1
    Interval Start:0 days 0 hours 52 minutes 59 seconds
    Utilization:0
    Rx statistics:
        Drop Events:0
        Octets:0
        Pkts:0
        Broadcast:0
        Multicast:0
        Jabbers:0
    Error statistics:
```

```
        CRC Errors:0
        Undersize:0
        Oversize:0
        Fragments:0
        Collisions:0
switch#
```

11.2.8 show rmon log

Function

The **show rmon log** command is used to show logs of RMON events.

Format

- **show rmon log**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

You can use this command to view log information of an RMON event, including the event ID, log ID, log recording time, and log description.

Example

Show logs of RMON events.

```
switch#show rmon log
  RMON Log:1/38
        Time:0 days 1 hours 35 minutes 23 seconds
        Description:alarm rising    1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
  RMON Log:1/39
        Time:0 days 1 hours 35 minutes 25 seconds
        Description:alarm rising    1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
  RMON Log:1/40
        Time:0 days 1 hours 35 minutes 27 seconds
        Description:alarm rising    1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
  RMON Log:1/41
```

```
        Time:0 days 1 hours 35 minutes 29 seconds
        Description:alarm rising    1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
  RMON Log:1/42
        Time:0 days 1 hours 35 minutes 31 seconds
        Description:alarm rising    1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
  RMON Log:1/43
        Time:0 days 1 hours 35 minutes 33 seconds
        Description:alarm rising    1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
  RMON Log:1/44
        Time:0 days 1 hours 35 minutes 35 seconds
        Description:alarm rising    1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
  RMON Log:1/45
        Time:0 days 1 hours 35 minutes 37 seconds
        Description:alarm rising    1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
  RMON Log:1/46
        Time:0 days 1 hours 35 minutes 39 seconds
        Description:alarm rising    1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
  RMON Log:1/47
        Time:0 days 1 hours 35 minutes 41 seconds
        Description:alarm rising    1,1.3.6.1.2.1.2.2.1.8.2,1,2,1
switch#
```

11.2.9 show rmon statistics

Function

The **show rmon statistics** command is used to show RMON statistics.

Format

- **show rmon statistics**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet and trunk), and interface group configuration view

Usage Guidelines

You can use this command to show the RMON statistics report, including the data source, Rx packets, all packets, and error packets.

Example

Show the RMON statistics report.

```
switch#show rmon statistics
  RMON Ethernet statistics 1
    Data Source:ifIndex.2
    Owner: N/A
    Status: valid
    Rx statistics:
        Drop Events: 0
        Octets: 62067
        Pkts: 396
        Broadcast: 19
        Multicast: 11
    Packets statistics:
        64 Octets: 506
        65-127 Octets: 216
        128-255 Octets: 8
        256-511 Octets: 0
        512-1023 Octets: 20
        1024-1518 Octets: 42
        Jabbers: 0
    Error statistics:
        CRC Errors: 0
        Undersize: 0
        Oversize: 0
        Fragments: 0
        Collisions: 0
switch#
```

11.3 SNMP Configuration Commands

11.3.1 show snmp agent

Function

The **show snmp agent** command is used to show SNMP agent information on a switch.

Format

- **show snmp agent**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

You can use this command to show SNMP agent information, including the contact information of the current device node, physical position of the current device node, interval for reporting trap messages, and whether trap reporting is enabled.

Example

Show SNMP agent information on a switch.

```
switch#show snmp agent
SNMP agent:
   location is Delaware-USA
   contact is Feisu Technologies co.,Ltd.
   auth-failure trap is enable
   Local EngineID:80000EDF03000567FC0000
   timertrap interval is 30 seconds
   timertrap is disable
   snmp trap-log priority is 5
   snmp trap-log action is history
switch#
```

11.3.2 show snmp community

Function

The **show snmp community** command is used to show the SNMP community configuration.

Format

- **show snmp community**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

You can use this command to view SNMP community configuration information, including the community name, access permissions, and state.

Example

Show the SNMP community configuration.

```
switch#show snmp community
  Community                        Privilege   Status   Filter      View
  $9$kijv$1cb644f2f3a47f03         ro          VALID    N/A         internet
switch#
```

11.3.3 show snmp config

Function

The **show snmp config** command is used to show the SNMP configuration.

Format

- **show snmp config**

Parameters

None

Default Value

None

View

Privileged user view and global configuration view

Usage Guidelines

You can use this command to show SNMP configurations with a configuration file.

Example

Show the SNMP configuration.

```
switch#show snmp config
 Software Version                : SNMP_VX2.11.00.00
 snmp community $9$kijv$1cb644f2f3a47f03 ro view internet
switch#
```

11.3.4show snmp group

Function

The **show snmp group** command is used to show SNMP group information.

Format

- **show snmp group**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

You can use this command to show SNMP group information, including the group name, readable view, and writable view.

Example

Show SNMP group information.

```
switch#show snmp group
Group                ReadView            WriteView           NotifyView
1                    sun333              sun333              sun333
switch#
```

11.3.5show snmp statistic

Function

The **show snmp statistic** command is used to show statistics on SNMP packet processing.

Format

- **show snmp statistic**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

You can use this command to analyze packet statistics and obtain information about communication between the switch and the NMS, facilitating fault identification.

Example

Show the statistics on SNMP packet processing.

```
switch#show snmp statistic
  snmpInPkts : 0
  snmpInBadVersions : 0
  snmpInBadCommunityNames : 0
  snmpInBadCommunityUses : 0
  snmpInASNParseErrs : 0
  snmpInBadTypes : 0
  snmpInTooBigs : 0
  snmpInNoSuchNames : 0
  snmpInBadValues : 0
  snmpInReadOnlys : 0
  snmpInGenErrs : 0
  snmpInTotalReqVars : 0
  snmpInTotalSetVars : 0
  snmpInGetRequests : 0
  snmpInGetNexts : 0
  snmpInSetRequests : 0
  snmpInGetResponses : 0
  snmpInTraps : 0
  snmpOutPkts : 0
  snmpOutTooBigs : 0
  snmpOutNoSuchNames : 0
  snmpOutBadValues : 0
  snmpOutReadOnlys : 0
  snmpOutGenErrs : 0
  snmpOutGetRequests : 0
  snmpOutGetNexts : 0
  snmpOutSetRequests : 0
  snmpOutGetResponses : 0
  snmpOutTraps : 0
  snmpUnknownSecurityModels : 0
  snmpInvalidMsgs : 0
```

```
  snmpUnknownPDUHandlers : 0
  snmpUnavailableContexts : 0
  snmpUnknownContexts : 0
  usmStatsUnsupportedSecLevels : 0
  usmStatsNotInTimeWindows : 0
  usmStatsUnknownUserNames : 0
  usmStatsUnknownEngineIDs : 0
  usmStatsWrongDigests : 0
  usmStatsDecryptionErrors : 0
switch#
```

11.3.6 show snmp trap-server

Function

The **show snmp trap-server** command is used to show the host that receives trap messages and its version.

Format

- **show snmp trap-server**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

You can use this command to check the host receiving trap messages and its version, including the host IP address, port number, version, and status.

Example

Show the host that receives trap messages and its version.

```
switch#show snmp trap-server
  IP-Address          Port   Ver Status     Level   Name
  1.1.1.1             162    V3  active     None    public
  2.3.1.2             162    V1  active     None    public
switch#
```

11.3.7 show snmp user

Function

The **show snmp user** command is used to show SNMP user information.

Format

- **show snmp user**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

You can use this command to show SNMP user information, including the user name, group name, and authentication status.

Example

Show SNMP user information.

```
switch#show snmp user
User                Group               Auth    Priv    Filter
U1                  group1              MD5     DES     N/A
switch#
```

11.3.8 show snmp view

Function

The **show snmp view** command is used to show SNMP view information.

Format

- **show snmp view**

Parameters

None

Default Value

None

View

Common user view, privileged user view and global configuration view

Usage Guidelines

None

Example

Show SNMP view information.

```
switch#show snmp view
View              Type         OidTree                Mask
V1                included   1.3.6.1.2.1.1            all-1
internet          included   1.3.6                    all-1
internet          excluded   1.3.6.1.6.3.15           all-1
internet          excluded   1.3.6.1.6.3.16           all-1
switch#
```

11.3.9snmp auth-trap

Function

The **snmp auth-trap** command is used to enable or disable the authentication trap.

Format

- **snmp auth-trap** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the authentication trap.	-
disable	Disables the authentication trap.	-

Default Value

By default, the authentication trap is enabled.

View

Global configuration view

Usage Guidelines

After the authentication trap is enabled, a switch sends a trap message if authentication fails.

Example

Disable the authentication trap.

```
switch(config)#snmp auth-trap disable
switch(config)#
```

11.3.10 snmp bulk max-varbind

Function

The **snmp bulk max-varbind** command is used to set the maximum number of variable bindings in an SNMP Get Bulk request.

Format

- **snmp bulk max-varbind** { *max-number* | **default** }

Parameters

Parameters	Description	Value
max-number	Specifies the maximum number of variable bindings in an SNMP Get Bulk request.	The value is an integer in the range from 100 to 4000.
default	Indicates the default.	512

Default Value

512

View

Global configuration view

Usage Guidelines

The number of variables collected by an SNMP Get Bulk message is N + (M x R), where N is the smaller one between the value of non-repeaters and the number of request variables, M is the value of max-repetitions, and R is the larger one between the number of request variables - N and 0.

Example

Set the maximum number of variable bindings in an SNMP Get Bulk request.

```
switch(config)#snmp bulk max-varbind 400
switch(config)#
```

11.3.11 snmp community

Function

The **snmp community** command is used to configure an SNMP community name.
The **no snmp community** command is used to delete an SNMP community name.

Format

- **snmp community** *name* { **ro** | **rw** }
- **snmp community** *name* { **ro** | **rw** } **view** *view-name*
- **no snmp community** *name*

Parameters

Parameters	Description	Value
name	Specifies a community name.	The value is a string of less than 20 characters.
{ **ro** | **rw** }	Indicates the permission of the community name in the specified view. The Parameters **ro** indicates the read-only permission and **rw** indicates the read-write permission.	-
view-name	Specifies the name of the view corresponding to the community name.	The value is a character string.

Default Value

The default SNMP community name can be **public** or **NETMAN**.

View

Global configuration view

Usage Guidelines

To remotely manage a switch using the SNMP NMS, you must set a community name. You can access the MIB information on a switch only after the community name passes the verification. If *view-name* is not specified, the system starts the access from the Internet node by default.

Example

Create a readable community named public.

```
switch(config)#snmp community public ro
switch(config)#
```

11.3.12 snmp contact

Function

The **snmp contact** command is used to configure the contact mode.

Format

- **snmp contact** *contact-info*

Parameters

Parameters	Description	Value
contact-info	Specifies the contact information for system maintenance.	The value is a character string.

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to configure the SNMP contact information, so that users can easily contact the device supplier.

Example

Configure the contact information 88888888.

```
switch(config)#snmp contact 88888888
switch(config)#
```

11.3.13 snmp fail-count

Function

The **snmp fail-count** command is used to set the number of SNMP authentication failures.

Format

- **snmp fail-count** *count*

Parameters

Parameters	Description	Value
count	Specifies the number of SNMP authentication failures.	The value is an integer in the range from 0 to 30.

Default Value

By default, the number of SNMP authentication failures is 0, indicating that the number of authentication attempts is not limited.

View

Global configuration view

Usage Guidelines

You can use this command to configure the number of continuous SNMP login failures. If the number of login failures reaches the specified value, a switch enters the silence period. Within this period, you cannot log into the switch using SNMP, until the silence period ends.

Example

Set the number of SNMP authentication failures to 6.

```
switch(config)#snmp fail-count 6
switch(config)#
```

11.3.14 snmp group

Function

The **snmp group** command is used to configure SNMP group information.
The **no snmp group** command is used to delete SNMP group information.

Format

- **snmp group** *group-name* **read-view** *read-view* **write-view** *write-view* **notify-view** *notify-view*
- **no snmp group** *group-name*

Parameters

Parameters	Description	Value
group-name	Specifies an SNMP group name.	The value is a string of no more than 32 characters.
read-view	Specifies a read-only view name.	The value is a character string.
write-view	Specifies a read-write view name.	The value is a character string.
notify-view	Specifies a notification view name.	The value is a character string.

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to configure SNMP group information, including the group name and read, write, or notification view name. Different SNMP users in the group are mapped to different views, so that these SNMP users are assigned with different access permissions.

Example

Configure a SNMP group 1. Set the read-only view name to sun333, read-write view name to sun333, and notification view to sun333.

```
switch(config)#snmp group 1 read-view sun333 write-view sun333 notify-view sun333
switch(config)#
```

11.3.15 snmp location

Function

The **snmp location** command is used to configure the location of a switch.

Format

- **snmp location** *location-info*

Parameters

Parameters	Description	Value
location-info	Specifies the location of a switch.	The value is a character string.

Default Value

The default location of a switch is Delaware**-USA**

View

Global configuration view

Usage Guidelines

You can use this command to configure the current location of a switch.

Example

Set the current location of a switch to Delaware-**USA**.

```
switch(config)#snmp location Delaware-USA
switch(config)#
```

11.3.16 snmp|snmp6 port

Function

The **snmp|snmp6 port** command is used to set the SNMP port number.

Format

- **snmp port** { *port-number* | **default** }
- **snmp6 port** { *port-number* | **default** }

Parameters

Parameters	Description	Value
port-number	Specifies the SNMP port number.	The value is an integer in the range from 1024 to 65535.
default	Indicates the default.	The value is 161.

Default Value

The default SNMP port number is 161.

View

Global configuration view

Usage Guidelines

None

Example

Set the SNMP port number to 1024.

```
switch(config)#snmp port 1024
switch(config)#
```

11.3.17 snmp reauth-interval

Function

The **snmp reauth-interval** command is used to set the SNMP re-authentication interval.

Format

- **snmp reauth-interval** *interval*

Parameters

Parameters	Description	Value
interval	Specifies the re-authentication interval.	The value is an integer in the range from 0 to 1440, in minutes.

Default Value

By default, the SNMP re-authentication interval is 0 minutes, indicating no silence time.

View

Global configuration view

Usage Guidelines

You can use this command to configure the number of continuous SNMP login failures. If the number of login failures reaches the specified value, a switch enters the silence period. Within this period, you cannot log into the switch using SNMP, until the silence period ends.

Example

Set the SNMP re-authentication interval to 10 minutes.

```
switch(config)#snmp reauth-interval 10
switch(config)#
```

11.3.18 snmp rw-community

Function

The **snmp rw-community** command is used to enable or disable the writing of an SNMP community name.

Format

- **snmp rw-community** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the writing of a community name.	-
disable	Disables the writing of a community name.	-

Default Value

By default, the writing of a community name is enabled.

View

Global configuration view

Usage Guidelines

None

Example

Disable the writing of a community name.

```
switch(config)#snmp rw-community disable
switch(config)#
```

11.3.19 snmp|snmp6 trap-server

Function

The **snmp|snmp6 trap-server** command is used to specify the address for receiving SNMP trap messages.
The **no snmp|snmp6 trap-server** command is used to delete a receiver.

Format

- **snmp trap-server** *ipv4-address security-name* { **v1** | **v2** | **v3** }
- **snmp trap-server** *ipv4-address port security-name* { **v1** | **v2** | **v3** }
- **snmp trap-server** *ipv4-address security-name* **v3** { **auth** | **priv** }
- **snmp trap-server** *ipv4-address port security-name* **v3** { **auth** | **priv** }
- **snmp6 trap-server** *ipv6-address security-name* { **v1** | **v2** | **v3** }
- **snmp6 trap-server** *ipv6-address port security-name* { **v1** | **v2** | **v3** }
- **snmp6 trap-server** *ipv6-address security-name* **v3** { **auth** | **priv** }
- **snmp6 trap-server** *ipv6-address port security-name* **v3** { **auth** | **priv** }
- **no snmp trap-server** *ipv4-address*
- **no snmp trap-server** *ipv4-address security-name*
- **no snmp6 trap-server** *ipv6-address*
- **no snmp6 trap-server** *ipv6-address security-name*

Parameters

Parameters	Description	Value
ipv4-address	Specifies the IPv4 address of the host used to receive trap messages.	The value is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of the host used to receive trap messages.	-
{ v1 | v2 | v3 }	Specifies the version number of SNMP trap messages.	-
security-name	Specifies a community name.	The value is a character string.
{ auth | priv }	Specifies the authentication or private mode.	-
port	Specifies the number of the port that sends trap messages.	The value is an integer in the range from 1 to 65535. The default is 162.

Default Value

None

View

Global configuration view

Usage Guidelines

To facilitate remote fault location on the switch, you can specify the IP address of a host to receive trap messages from the switch.

Example

Configure the switch to send trap messages to the host with IP address 10.5.6.8 and running SNMP version v2.

```
switch(config)#snmp trap-server 10.5.6.8 name123 v2
switch(config)#
```

11.3.20 snmp trap-source

Function

The **snmp trap-source** command is used to set the source IP address for sending SNMP trap messages.
The **no snmp trap-source** command is used to delete the configuration.

Format

- **snmp trap-source** *ipv4-address*
- **no snmp trap-source**

Parameters

Parameters	Description	Value
ipv4-address	Specifies a source IPv4 address.	The value is in dotted decimal notation.

Default Value

None

View

Global configuration view

Usage Guidelines

You can specify the source IP address for sending SNMP trap messages as required. The specified source IP address must exist on the switch. Once configured, all trap messages sent from the switch use this IP address as the source IP address. If you do not specify it, trap messages carry the actual IP address where they are sent. For example, an interface of an L3 switch may have multiple VLAN interface IP addresses. When the physical port generates a link up or link down alarm, there may be multiple source IP addresses in the alarm. You can use this command to designate a source IP address in the alarm message.

Example

Set the source IP address for sending SNMP trap messages to 1.1.1.1.

```
switch(config)#snmp trap-source 1.1.1.1
switch(config)#
```

11.3.21 snmp user

Function

The **snmp user** command is used to create an SNMP user.
The **no snmp user** command is used to delete an SNMP user.

Format

- **snmp user** *user-name* **group** *group-name* **no-auth-no-priv**
- **snmp user** *user-name* **group** *group-name* **auth** { **md5** | **sha** } *authkey* **priv no-priv**
- **snmp user** *user-name* **group** *group-name* **auth** { **md5** | **sha** } *authkey* **priv des** *privkey*
- **no snmp user** *user-name*

Parameters

Parameters	Description	Value
user-name	Specifies a user name.	The value is a string of no more than 32 characters.
group-name	Specifies a group name.	The value is a character string.
{ md5 | sha }	Sets the authentication mode to MD5 or SHA.	-
authkey	Specifies an authentication key.	The value is a character string.
privkey	Specifies an encryption key.	The value is a character string.
no-priv	Indicates encryption.	-
no-auth-no-priv	Indicates no authentication or encryption.	-

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to configure the SNMP user information, including the user name, group, authentication mode and encryption mode (authentication and encryption, authentication but no encryption, and no authentication and no encryption).

Example

Create a user named sun1. Set the group to group 1 and authentication mode to MD5.Set the authentication key to 0x1df745c352cc24781465e1a025ad1.Set the encryption key to 0xaaaf45e7357c629b97b7a36c526d5.

```
switch(config)#snmp user sun1 group 1 auth md5 0x1df745c352cc24781465e1a025ad1 priv des 0xaaaf45e7357c629b97b7a36c526d5
switch(config)#
```

11.3.22 snmp version

Function

The **snmp version** command is used to set the SNMP version.
The **no snmp version** command is used to cancel the configured SNMP version.

Format

- **snmp version** { **v1** | **v2** | **v3** | **all** }
- **no snmp version** { **v1** | **v2** | **v3** | **all** }

Parameters

Parameters	Description	Value
v1|v2|v3|all	Indicates v1, v2, v3, or all versions.	-

Default Value

By default,the snmp version is configurated as version all.

View

Global configuration view

Usage Guidelines

None

Example

Set the supported SNMP version to v3.

```
switch(config)#snmp version v3
switch(config)#
```

11.3.23 snmp view

Function

The **snmp view** command is used to configure the SNMP view.
The **no snmp view** command is used to delete a configured SNMP view.

Format

- **snmp view** *view-name oid-tree* { **included** | **excluded** }
- **snmp view** *view-name oid-tree* { **included** | **excluded** } **mask** *subtreemask*
- **no snmp view** *view-name*

- **no snmp view** *view-name oid-tree*

Parameters

Parameters	Description	Value
view-name	Specifies a view name.	The value is a string of no more than 32 characters.
oid-tree	Specifies the OID character string, used to identify the view range.	The value is a character string.
{ included | excluded }	Indicates the including or excluding relation.	-
subtreemask	Specifies the mask OID character string.	The value is a character string.

Default Value

None

View

Global configuration view

Usage Guidelines

You can use this command to configure the SNMP view. It is applicable to SNMPv3. Specifying the access range of a view can improve the security and controllability.

Example

Configure a SNMP view v3view and set the access range to include the content of 1.3.6.1MIB.

```
switch(config)#snmp view v3view 1.3.6.1 include
switch(config)#
```

11.4 LLDP Configuration Commands

11.4.1 lldp tx-interval

Function

The **lldp tx-interval** command is used to set the LLDP frame transmission interval.

Format

- **lldp tx-interval** { *tx-interval* | **default** }

Parameters

Parameters	Description	Value
tx-interval	Specifies the LLDP frame transmission interval, in seconds.	The value is an integer in the range from 5 to 32768.

Parameters	Description	Value
default	Indicates the default.	30 seconds

Default Value

30 seconds

View

Global configuration view

Usage Guidelines

None

Example

Set the LLDP frame transmission interval to 10 seconds.

```
switch(config)#lldp tx-interval 10
switch(config)#
```

11.4.2lldp tx-hold

Function

The **lldp tx-hold** command is used to set the multiplier of LLDP frame transmission interval.

Format

- **lldp tx-hold** { *tx-hold* | **default** }

Parameters

Parameters	Description	Value
tx-hold	Specifies the multiplier of LLDP frame transmission interval.	The value is an integer in the range from 2 to 10.
default	Indicates the default.	4

Default Value

4

View

Global configuration view

Usage Guidelines

None

Example

Set the multiplier of LLDP frame transmission interval to 5.

```
switch(config)#lldp tx-hold 5
switch(config)#
```

11.4.3lldp reinit-delay

Function

The **lldp reinit-delay** command is used to set the delay in re-initiating the LLDP interface status.

Format

- **lldp reinit-delay** { *delay* | **default** }

Parameters

Parameters	Description	Value
delay	Specifies the delay in re-initiating the LLDP interface status.	The value is an integer in the range from 1 to 10.
default	Indicates the default.	2 seconds

Default Value

2 seconds

View

Global configuration view

Usage Guidelines

None

Example

Set the delay in re-initiating the LLDP interface status to1 seconds.

```
switch(config)#lldp reinit-delay 1
switch(config)#
```

11.4.4lldp tx-delay

Function

The **lldp tx-delay** command is used to set the delay in sending LLDP packets.

Format

- **lldp tx-delay** { *tx-delay* | **default** }

Parameters

Parameters	Description	Value
tx-delay	Specifies the delay in sending LLDP packets.	The value is an integer in the range from 1 to 8192.
default	Indicates the default.	2 seconds

Default Value

2 seconds

View

Global configuration view

Usage Guidelines

This command sets the minimum delay before an interface module sends LLDP packets to the neighbor when the LLDP status of the switch changes frequently.

Example

Set the delay in sending LLDP packets to 5 seconds.

```
switch(config)#lldp tx-delay 5
switch(config)#
```

11.4.5lldp notification-interval

Function

The **lldp notification-interval** command is used to set the global trap transmission interval.

Format

- **lldp notification-interval** { *interval* | **default** }

Parameters

Parameters	Description	Value
interval	Specifies the trap transmission interval.	The value is an integer in the range from 5 to 3600.
default	Indicates the default.	5 seconds

Default Value

5 seconds

View

Global configuration view

Usage Guidelines

When traps are generated because of frequent state changes on a switch, the switch sends a trap only when the interval between two traps is longer than the configured interval.

Example

Set the trap transmission interval to 6 seconds.

```
switch(config)#lldp notification-interval 6
switch(config)#
```

11.4.6lldp admin-status

Function

The **lldp admin-status** command is used to enable LLDP and set its administrative status or disable LLDP at an interface.

Format

- **lldp admin-status** { **tx-only** | **rx-only** | **rx-tx** | **disable** }

Parameters

Parameters	Description	Value
tx-only	Sends LLDP packets only.	-
rx-only	Receives LLDP packets only.	-
rx-tx	Sends and receives LLDP packets.	-
disable	Neither sends nor receives LLDP packets.	-

Default Value

The local LLDP agent can neither transmit or receive LLDP frames.

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

None

Example

Set the LLDP administrative status.

```
switch(config-100ge1/0/1)#lldp admin-status tx-only
switch(config-100ge1/0/1)#
```

11.4.7lldp notification {enable|disable}

Function

The **lldp notification {enable|disable}** command is used to enable or disable the LLDP alarm function at an interface.

Format

- **lldp notification** { **enable** | **disable** }

Parameters

Parameters	Description	Value
enable	Enables the LLDP alarm function at an interface.	-
disable	Disables the LLDP alarm function at an interface.	-

Default Value

By default, the LLDP alarm function is disabled at an interface.

View

Interface configuration view (Ethernet) and interface group configuration view

- Usage **Guidelines**

None

Example

Enable the LLDP alarm function at an interface.

```
switch(config-100ge1/0/1)#lldp notification enable
switch(config-100ge1/0/1)#
```

11.4.8lldp management-address

Function

The **lldp management-address** command is used to set the LLDP management IP address.

Format

- **lldp management-address** *ip-address* { **enable** | **disable** }
- **lldp management-address** *mac-address* { **enable** | **disable** }

Parameters

Parameters	Description	Value
ip-address	Specifies an IP address.	The value is in dotted decimal notation.
mac-address	Specifies a MAC address.	The value is in the format of AA:BB:CC:DD:EE:FF, where each of the letters A to F represents a hexadecimal digit.
enable	Enables the LLDP management IP address.	-
disable	Disables the LLDP management IP address.	-

Default Value

disable

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

None

Example

Set the LLDP management IP address.

```
switch(config-100ge1/0/1)#lldp management-address 1.2.3.1 enable
switch(config-100ge1/0/1)#
switch(config-100ge1/0/1)#lldp management-address 00:00:00:ee:ff:ab enable
switch(config-100ge1/0/1)#
```

11.4.9lldp basic-tlv-tx

Function

The **lldp basic-tlv-tx** command is used to set the basic LLDP TLV at an interface.

Format

- **lldp basic-tlv-tx** { **port-description** | **system-name** | **system-description** | **system-capability** | **all** } { **enable** | **disable** }

Parameters

Parameters	Description	Value
port-description	Indicates a port description.	-
system-name	Indicates a system name.	-

Parameters	Description	Value
system-description	Indicates a system description.	-
system-capability	Indicates a system capability.	-
all	Indicates all the preceding items.	-
enable	Enables the basic LLDP TLV at an interface.	-
disable	Disables the basic LLDP TLV at an interface.	-

Default Value

enable

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

None

Example

Configure the basic LLDP TLV.

```
switch(config-100ge1/0/1)#lldp basic-tlv-tx port-description enable
switch(config-100ge1/0/1)#
```

11.4.10 reset lldp counter

Function

The **reset lldp counter** command is used to reset the LLDP interface statistics.

Format

- **reset lldp counter**

Parameters

None

Default Value

None

View

Interface configuration view (Ethernet) and interface group configuration view

Usage Guidelines

None

Example

Reset the LLDP interface statistics.

```
switch(config-100ge1/0/1)#reset lldp counter
switch(config-100ge1/0/1)#
```

11.4.11 show lldp interface

Function

The **show lldp interface** command is used to show LLDP interface information.
The **show lldp interface verbose** command is used to show detailed LLDP interface information.

Format

- **show lldp interface**
- **show lldp interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*
- **show lldp interface verbose**

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of 1-1 / 0-2 / 1-52.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet), and interface group configuration view

Usage Guidelines

None

Example

Show LLDP interface information.

```
switch(config)#show lldp interface 10gigaethernet 1/0/1
  Port 100ge-1/0/1:
        Admin status:Disable
switch(config)#
```

11.4.12 show lldp statistic

Function

The **show lldp statistic** command is used to show LLDP statistics.
The **show lldp statistic interface** command is used to show LLDP statistics at an interface.

Format

- **show lldp statistic**
- **show lldp statistic interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of 1-1 / 0-2 / 1-52.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet), and interface group configuration view

Usage Guidelines

None

Example

Show LLDP statistics.

```
switch#show lldp statistic
LLDP statistic:
  LLDP Msap statistic:
        Last change-time: 0 days 0 hours 0 minutes 0 seconds
        Inserts:0
        Deletes:0
        Drops:0
        Ageouts:0(s)

  LLDP port statistic:
switch#
```

11.4.13 show lldp remote

Function

The **show lldp remote** command is used to show information about all neighbors or a specified neighbor.

Format

- **show lldp remote**
- **show lldp remote verbose**
- **show lldp remote** *remote-number*

Parameters

Parameters	Description	Value
remote-number	Specifies a neighbor ID.	The value is an integer in the range from 1 to 2147483647.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet), and interface group configuration view

Usage Guidelines

None

Example

Show information about all neighbors.

```
switch#show lldp remote
switch#
```

11.4.14 show lldp local

Function

The **show lldp local** command is used to show local LLDP device information.

Format

- **show lldp local**

Description

None

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet), and interface group configuration view

Usage Guidelines

None

Example

Show local LLDP device information.

```
switch(config)#show lldp local
  LLDP local:
        Message tx-interval:30(s)
        Message tx-hold:4
        Reinit delay:2(s)
        Tx delay:2(s)
        Notification interval:10(s)
        Chassis type:MAC Address
        Chassis ID:0004:0290:ffff
        System name:switch
        System desc:Feisu Routing Switch
        System supported:Bridge/Switch,Router
        System capenabled:Bridge/Switch,Router

        Med information:
        Device class:Network Connectivity Device
        Faststart repeat-count:1
        Hardware revision:1.0
        Firmware revision:0.1
        Software revision:V210R230
        Serial number:-
        Manufacturer name:Feisu
        Model name:LLDP
        Asset ID:N/A
        POE type:pse
switch(config)#
```

11.4.15 show lldp config

Function

The **show lldp config** command is used to show the LLDP configuration.

Format

- **show lldp config**

Parameters

None

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet), and interface group configuration view

Usage Guidelines

None

Example

Show the LLDP configuration.

```
switch(config)#show lldp config
 lldp notification-interval 10
 lldp faststart-count
switch(config)#
```

11.4.16 show lldp remote interface

Function

The **show lldp remote interface** command is used to show the neighbor information at an interface.

Format

- **show lldp remote interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of 1-1 / 0-2 / 1-52.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet), and interface group configuration view

Usage Guidelines

None

Example

Show the neighbor information at an interface.

```
switch#show lldp remote interface 10gigaethernet 1/0/1
switch#
```

11.4.17 show lldp config interface

Function

The **show lldp config interface** command is used to show the LLDP configuration at an interface.

Format

- **show lldp config interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of 1-1 / 0-2 / 1-52.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet), and interface group configuration view

Usage Guidelines

None

Example

Show the neighbor information at an interface.

```
switch(config)#show lldp config interface 10gigaethernet 1/0/1
```

```
interface 10gigaethernet 1/0/1
lldp med-notification enable
switch(config)#
```

11.4.18 show lldp local interface

Function

The **show lldp local interface** command is used to show information about a local LLDP interface.

Format

- **show lldp local interface** { **10gigaethernet** | **100gigaethernet** } *interface-number*

Parameters

Parameters	Description	Value
interface-number	Specifies an Ethernet interface number.	The value is an integer in the range of 1-1 / 0-2 / 1-52.

Default Value

None

View

Common user view, privileged user view, global configuration view, interface configuration view (Ethernet), and interface group configuration view

Usage Guidelines

None

Example

Show information about a local LLDP interface.

```
switch#show lldp local interface 10gigaethernet 1/0/1
switch#
```

https://www.fs.com

The information in this document is subject to change without notice. FS has made all efforts to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty.

Copyright © 2009-2022 FS.COM All Rights Reserved.